State of Washington Windows 2000
Root Domain Requirements

Project:	State of Washington Multi-Agency Forest Project
Title:	Root Domain Requirements
Version:	1.0
Status:	Approved
Date:	May 4, 2001

Revision History

Version	Date	Comments
0.1	March 28 2001	Combined numerous documents into one - AD Architecture Components (Approved by Development Group) - Firewall Requirements for the root (Approved by Development Group) - Essential Security Items (Approved by Development Group) - Procedures for Test root - Procedures for Production root - Backup Restore procedures Sent to Dev Group on March 29 2001
0.2	March 30 2001	Updated Firewall section based on dev group and ESS approval
0.3	April 2 2001	Added Sites Section and DNS section and approved by Development Group
0.4	April 4 2001	Made changes to Sites and DNS sections per Development Group
0.4a,b	April 4, 2001	Updated sites diagram

Contributors

Authors: John Sadie (DSHS – State of WA), Scott Rehm (LNI – State of WA), Jay Knowlton (DSHS – State of WA), John Ditto (DIS – State of WA), Brent McCarthy (Microsoft Consulting Services), Krishnan P Iyer (Microsoft Consulting Services).
Reviewers: Lance Calish (DIS – State of WA), John Odegaard (LNI – State of WA), Keith Kawamura (GA – State of WA), David Salang (DOP – State of WA), Bill Davis (DFI – State of WA), Mike Frost (DSHS – State of WA), Dennis Trout (EMD – State of WA), Larry Colbert (ESD – State of WA) Robin Japhet (GA – State of WA), Chuck Moore (DIS – State of WA), Jane Rasmussen (Microsoft Consulting Services), Chris Whitney (Microsoft Product Support Services), and other members of the Win2K development group.
Approvers: State of WA - Windows 2000 Development Group, State of WA - Windows 2000 Steering Committee

Table of Contents

Windows 2000 Active Directory Architecture Components

Introduction

This section summarizes the items that are needed for the Windows 2000 (Win2K) forest root single domain to be up and running at the State of WA by April 30th. It details the (Active Directory) AD architecture components required to complete Phase 1 - 'Root requirements' as described in the Summary Project Plan. This section only identifies the decisions made regarding the key components required and does not attempt to describe how the technology operates. Refer to (http://www.microsoft.com/windows2000) for documents like white papers, best practices, product guides, tools and resources, technical library on Windows 2000.

These recommendations below have been reviewed / approved by the Windows 2000 Development Group at the State of Washington.

Root and Forest Name

The State of Washington will use the root name WA.LCL for its Windows 2000 production forest and the root name WA.TST for its Windows 2000 test forest Refer to the "Naming Convention Document" for more information.

Authoritative Time Servers for the Windows 2000 forest

The root domain will use the Simple Network Time Protocol (SNTP) time servers run by the U.S. Naval Observatory. The root domain will use the Microsoft Knowledge Base article Q216734 which describes how to configure an authoritative Time Server in Windows 2000. All the child domains will use the State Windows 2000 root domain to synchronize their time. A similar mechanism is being used now indicating that no additional firewall work will be needed since the firewalls are already allowing this kind of information through.

Licensing Logging for the root domain will be left as default. Windows 2000 uses Sites to collect and track Licensing information. This will allow each agency to track their available and used licenses based on Agency licenses. Please refer to Microsoft Knowledge base article Q273475 for Licensing in Windows 2000 and Differences with Windows NT 4.0.

Organizational Unit (OU) Structure for root domain

The State of Washington will use the default OU's created in the Windows 2000 root domain. After April 30, 2001 this will be updated to reflect any changes that might be needed.

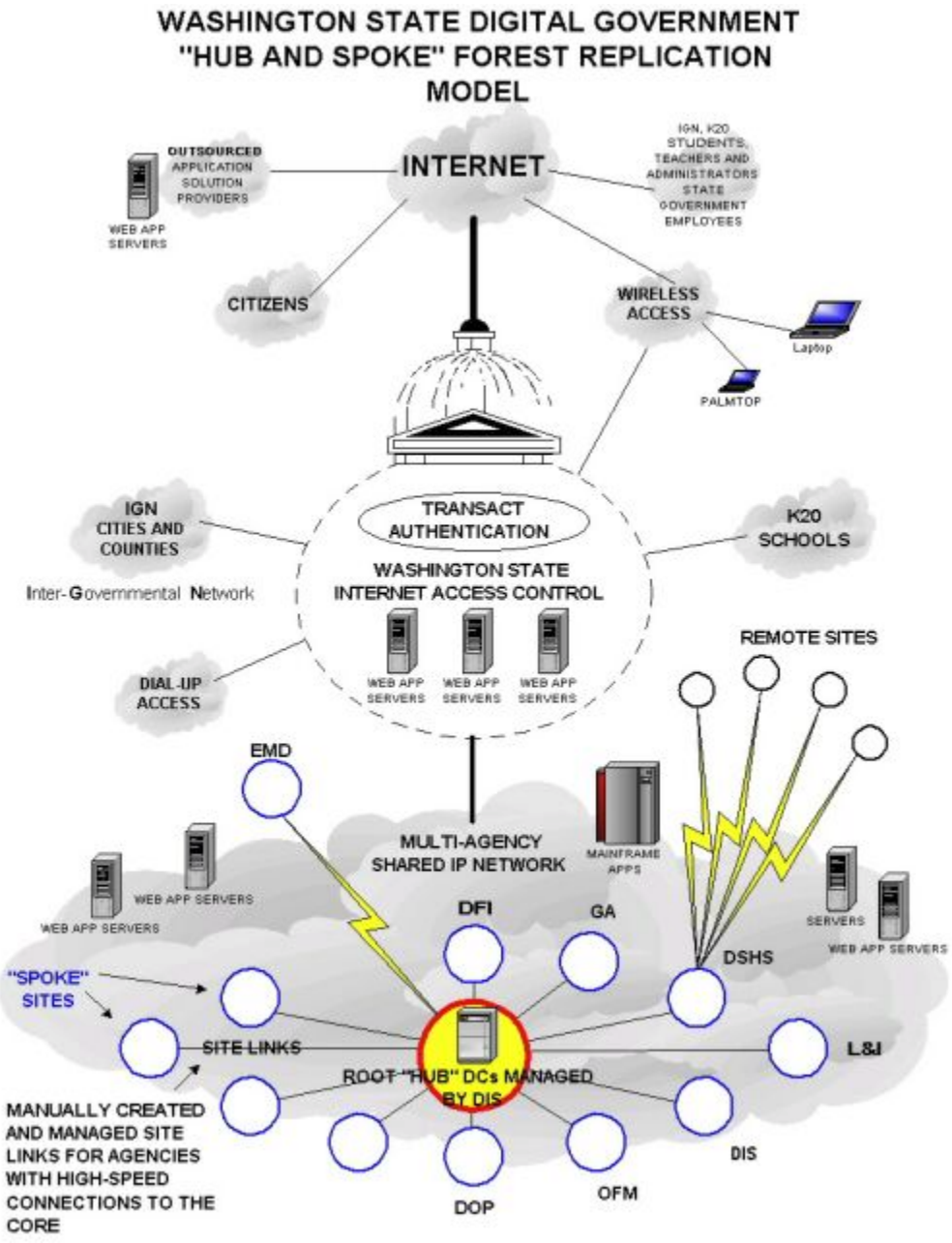
Site Topology for the root

State of Washington will use two sites for the root domain. That will be called *WAoly0001* and *WAspo0001.*

The name of a directory object does not reflect the site or sites in which the object is stored. A site may contain DC's from several domains, and DC's from a domain may be present in several sites. A Windows 2000 site represents a region of uniformly good network access, which can be interpreted as being generally equivalent to local area network (LAN) connectivity. This section documents the Hub and Spoke model approved by the development group April 2, 2001.

Hub and Spoke model

A logical topology for the State of WA is the hub and spoke design depicted in the following drawing. The Knowledge Consistency Checker (KCC) will be disabled for Inter-site Replication and enabled for intra site replication. Refer to Microsoft Knowledge Base Article Q245610.



Some advantages of the Hub and Spoke model to the State of WA are:

- Manageability. This would allow us to manage replication schedules to minimize any adverse effects that replication might have on the members of the statewide forest. By manually creating connections to and from the forest “Root” servers, replication of objects to and from the forest can be scheduled to off peak hours. This allows an agency’s global catalog servers to handle its’ primary functions of authentication, LDAP searches and replication of the agency’s domain data during

normal business hours.

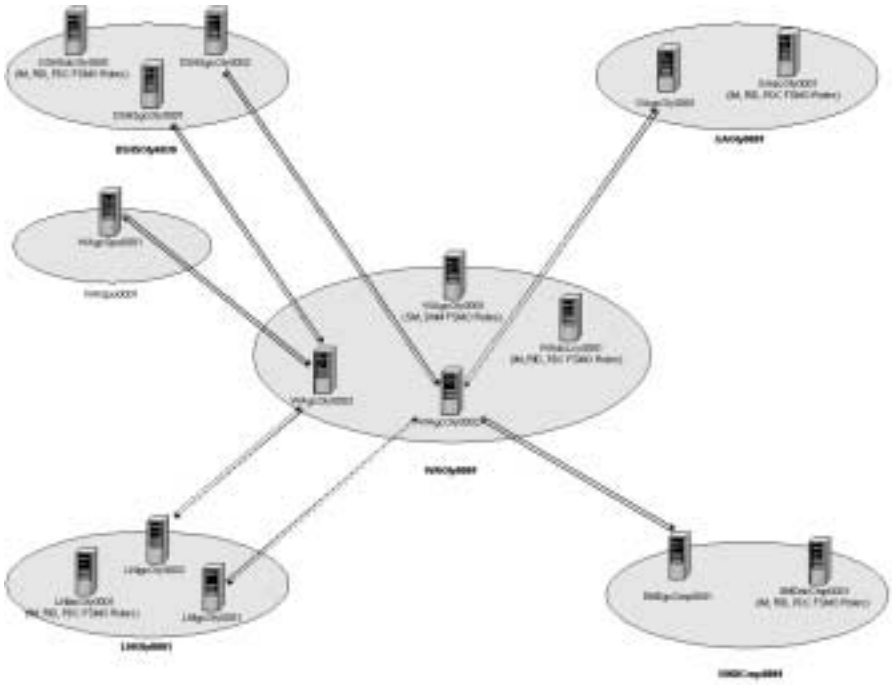
- Replication control. By changing the replication schedule associated with a site link or connection object, an agency or DIS would be able to control the replication occurring to or from the forest (global catalog data). For instance if a large agency was forced to do an authoritative restore during the day, every object (partial attributes) would be replicated to every global catalog server in the forest. This replication may not be desirable during normal business hours and could be controlled by disabling replication from that domain for a predetermined period of time.
- Load balancing. Monitoring and balancing the load put on any given bridgehead server in the “Root” site is another advantage of this model over a KCC generated replication topology.

Some disadvantages of the Hub and Spoke model to the State of WA are:

- Replication latency. Replication within a site is driven by changes but in this model they are driven by a schedule. The replication that we are talking about in this case is inter-domain, only a partial replica of each domain (the global catalog) is being replicated. It may be acceptable for some amount of latency to occur with respect to the replication of objects belonging to other domains.
- Requires manual creation and management of connection objects and replication schedules between the “Root” bridgehead servers and an agency’s bridgehead servers. An agency would have to work with DIS to create a replication schedule and coordinate the creation of connection objects to and from the root.
- Replication topology (spoke and hub) is less efficient than the KCC generated (a bi-directional ring). It will require multiple “Root” bridgehead servers to allow for replication load balancing and redundancy.

The following drawing is an example of what a spoke and hub topology would look like. Represented in this drawing are the “Root” site “WAOly0001” and additional Windows 2000 sites representing different agency’s bridgehead servers and domain controllers. There are five Operations Master roles in the root domain, the two enterprise wide Operations Master roles (Schema Master and Domain Naming Master), and the three domain-wide Operations Master roles (PDC Emulator, Infrastructure Master and RID Master). Since the root domain is a small domain, the roles will not create a lot of load on the Operations Master role holders. Therefore, it is not necessary to plan for distributing these roles to different domain controllers, except to ensure that the Infrastructure Master is not a global catalog server.

The other thing to observe in this drawing are the “site-links” represented by the connection objects between Windows 2000 sites. First, there are no site-links between bridgehead servers from agency to agency. The only connections are agency bridgehead servers to bridgehead servers in the “Root” site. This means that all changes made in the “LNI” domain will be replicated to the other domains in a transitive nature through replication from “LNI” to the “Root” and in turn from the “Root” to the other domains on a pre-determined schedule. You should also note the site-links, which vary from a single site-link to multiple site-links between sites. A single site-link is all that is necessary for replication to occur, but multiple site-links provide fault tolerance and load balancing. For example, the 2 site links that are documented below are on different schedules. This automatically balances the load on the “Root” GCs and additionally, if one of the “Root” or agency servers were to fail, the load on the remaining server remains unchanged but now the servers get their replication updates once a day instead of twice daily.



In order to create a replication topology of this nature, we will have to disable the KCC and manually create connections to and from the “Root” bridgehead servers. This is the preferred method in configurations with hundreds of sites due to the KCC’s inability to scale. When automatic inter-site topology generation is disabled entirely, it becomes the responsibility of the administrators to create the necessary inter-site replication connection objects to ensure that replication data continues to flow across the forest. It is recommended that organizations with enough sites to surpass the KCC limits employ hub-and-spoke network topologies because this symmetry greatly simplifies the process.

Change Control for Sites

Active directory site topology determines how replication is handled. Each agency will create at least one site, which is separate from the forest root. (Note by default, the child domain joins the forest root's site). The agency will be responsible for configuring Windows 2000 so that it limits authentication traffic to within their own domain (with the exception of global catalog replication).

For connection to the Root each Agency will need to contact the Root Administrators for the root domain controller information.

The root administrators will keep the Change Management document. Changes to this document will be submitted to the Root Administrators Group for approval.

Any changes (adds/deletes/updates) to sites will be submitted to the Root Administrators for approval 10 working days prior to the scheduled change. The Root Administrators will disseminate site changes to all domain administrators.

The Child Domain Administrators will administer site and Site Links within Child Domains. Child Domain Administrators Group will be delegated the rights for managing sites within the domain.

Flexible Single Master Operations (FSMO) Roles and Global Catalog Location

The state will assign FSMO roles to the DC's in the root. Microsoft Knowledge base (KB) article Q223346 has details on how to assign these roles.

The State of WA will have 3 DC's in the root domain and the functions will be assigned as follows:

DOMAIN CONTROLLER	**FUNCTIONS**	**LOCATION**
WAgcOly0001	Schema Master and Domain Naming (GC Server) Master	Olympia
WAdcLcy0001	RID + PDC Roles, Infrastructure Master Roles, AD Backup.	Lacey
WAgcSpo0001	Global Catalog & natural disaster backup Server	Spokane
WAgcOly0003	Global Catalog & Bridgehead Server	Olympia

WagcOly0002	Global Catalog & Bridgehead Server	Olympia

IP Addressing & Domain Name Service

The root DC's will be using static IP addresses.

DNS for the Root Domain

The Forest Root domain will use the DNS server provided with Windows 2000.

The Forest Root DNS will be authoritative for the root (wa.lcl) domain only. Zone Authority for child domains will be delegated to the child domain's DNS.

The Forest Root DNS must be Active Directory integrated. (Default on first server)
- Simpler Management -Eliminates the need for managing two replication schedules.
- Fault Tolerance – MultiMaster Replication.
- Gives ability for (Secure) Dynamic Updates.

Aging/Scavenging must be left turned off (default).
- All hosts in the Dedicated Root Domain should be static. The Aging/Scavenging process is unnecessary and therefore should be left turned off to avoid any potential problems and unnecessary utilization of resources.

There should not be a DHCP server in the dedicated forest root domain. All IP addressing should be strictly controlled.
- This is an extra precaution against accidental/improper record registrations in the root namespace.

DNS must be tested for proper configuration.
- Proper record registrations (A, NS, SOA, PTR, SVR, CNAME).
- Forward and Reverse lookups.

There will be a minimum of two DNS servers in the root domain. They will be in physically separate subnets and in geographically separate locations.

The root DC's will be using AD integrated DNS, there will be two DNS servers

WAdcOLY0001 – DNS Primary
WAgcLCY0001- DNS Secondary

ACL's (Access Control Lists) must be modified to prevent anyone other than qualified DNS Administrators from adding records to the Forest Root DNS zone

Disaster Recovery Backup/Restore plan – DNS is Active Directory Integrated. Refer to Active Directory Disaster Recovery.

Here are some examples

Domain Controller	DNS Version	Zone Authority for	Zone Database Storage	Allow Dynamic Updates Configuration	Aging - Scavenging Configuration
WAdcOly0001	Windows 2000 DNS	wa.lcl	Active Directory Integrated	Do Not Accept Updates	Disabled (Default)
WAgcLcy0001	Windows 2000 DNS	wa.lcl	Active Directory Integrated	Do Not Accept Updates	Disabled (Default)

DNS for the Child Domain(s)

Child Domains must use the DNS server provided with Windows 2000 for Phase 1 (April 30, 2001)

The Child Domains DNS will be authoritative for the child (child.wa.lcl) domain and sub-domains only. Zone Authority for the Child DNS namespace will be delegated from the root (wa.lcl) DNS namespace.

The Child Domains DNS must be Active Directory Integrated for Phase 1 (April 30, 2001)

- Simpler Management -Eliminates the need for managing two replication schedules
- Fault Tolerance – MultiMaster Replication
- Gives ability for (Secure) Dynamic Updates.

The Child Domains DNS Aging/Scavenging[1] must be turned on.
*** Manually created (static) RR's should be examined carefully to make sure that they will be ignored by the Aging/Scavenging process. The Aging/Scavenging process will ignore RR's with a time stamp of zero. ***

The Child Domains DNS must be configured to accept Secure Dynamic Updates[2].
- <Add the client changes from Jay Knowlton for Ph2>
- Minimizes the possibility of name Hijacking.

[1] Refer to Page 412 (Chapter 6) of the Windows 2000 Server Resource Kit book before doing so.
[2] Refer to Page 391 of the Windows 2000 Server Resource Kit book.

- Protects DNS records from being improperly modified by enabling the application of ACL's to zones and resource records.

DNS must be tested for proper configuration.
- Proper record registrations (A, NS, SOA, PTR, SVR, CNAME)
- Forward and Reverse lookups

DNS must have Forwarders configured to point to the Root.
- In order for your Agency to be able to resolve DNS Records in the Root, as well as any other Agency, DNS Forwarding must be enabled, pointing to the Root DNS.

It is recommended that there be a minimum of two DNS servers in the child domain. Having them in physically separate subnets and in geographically separate locations is highly recommended[3].

Active Directory Communication in a Secured Firewall Environment

Introduction

In order to ensure security on the State Network, Firewalls are implemented between some agencies to maintain security boundaries and minimize security risks. This poses a challenge in the replication of Active Directory between sites that are secured by Firewalls. Some configuration is needed at the Firewalls and at the Domain Controllers to allow the bridgehead servers to authenticate, and replicate the information that Active Directory needs in order to have the current Forest information. The configuration that will enable this communication opens only 2 ports on the firewall, and allows the Bridgehead Domain Controllers to communicate securely by encrypting all communications between them with IP security (IPSec). This configuration also allows the Bridgehead servers to communicate openly on any port, as long as the data traffic is encrypted. It also adds an extra layer of security to the Windows 2000 Architecture in that all communications between sites would be encrypted.

Configuration (Encrypted IPSec)

This Configuration adds encrypted security using IPSec to the communication and replication between Domain Controllers in the Root and Child Domains. IP Security (IPSec) will cause performance overhead on the Domain Controllers that communicate using IPSec because of the extra processing required to

[3] Refer to the appendix in this document for Best Practices with DNS.

encrypt and decrypt the IP packets. There are hardware solutions that can offset this processing, which are Network Interface Cards with IPSec Co-Processors. These cards are currently available as 100Mbit PCI Ethernet controllers. The path throughput between replicating DCs is likely to be less than the maximum transmission rate of the IPSec offload in hardware (approx 85Mbits/sec). Thus with the IPSec hardware acceleration, IPSec encryption imposes no throughput overhead.

In order to use IPSec without implementing a Certificate Authority, Windows 2000 uses the Kerberos Authentication Protocol to authenticate the standard IKE RFC 2409 negotiation. Kerberos is the default authentication protocol for Windows 2000, so no extra protocols or services are required for Windows 2000 machines to negotiate IPSec communications.

By using this configuration, all ports would be available between the Bridgeheads and the Root Domain Controllers. The Firewall will allow all IPSec traffic, and would allow the domain controller to use any port they want as long as the data is encrypted using IPSec.

Firewall Configuration:

A. In order to pass IPSec traffic across a firewall, you must first open the following ports:

    1. TCP and UDP Port 88 (Kerberos Authentication)
    2. UDP Port 500 (Internet Key Exchange – IKE)

B. After the previous ports have been opened you must allow the use of the ESP Protocol (Encapsulating Security Protocol), Protocol ID 50 between the bridgehead servers in the Child Domains, and the Root Domain Controllers.

An example of a Firewall Conduit configuration is:

If the Child Domain Bridgehead had an IP address of 192.168.1.10,
And the Root Domain Controller had an IP address of 192.168.10.20,
The conduit list would look like this:

```
Conduit Permit TCP 192.168.1.10  eq 88 HOST 192.168.10.20
Conduit Permit UDP 192.168.1.10  eq 88 HOST 192.168.10.20
Conduit Permit UDP 192.168.1.10  eq 500 HOST 192.168.10.20
Conduit Permit ESP 192.168.1.10 HOST 192.168.10.20
```

Domain Controller Configuration:

In order for a Windows 2000 Server to communicate using IPSec, you must first apply an IPSec Policy to the server telling it when to use IPSec, and what Protocols to secure. You must also define the scope of the policy and when it will request to use IPSec.

IPSec Policies:

1. Client: Never requests to communicate using IPSec, but if a server makes the request of the client, it will communicate with IPSec.

2. Server: Will always request that IPSec be used in communications, but if the client is configured not to, then the server will not require the communications to be sent over IPSec.

3. Secure Server: Will only communicate using IPSec. Secure Server does not allow any other communication.

The IPSec Policy can be applied in two different places.

1. Group Policy: IPSec Policy can be applied using Group Policies to the Domain Controllers Organizational Unit.

2. Local Security Policy: This must be configured specifically on every Domain Controller that you want to use the IPSec Policy.

The Domain Controllers should use the “Server” Policy for IPSec, so that when these servers communicate together they are using IPSec, but can communicate in clear text with client desktops. The IPSec Policy should be edited to use IPSec only when it communicates with the IP addresses of other Domain Controllers to ensure that it is using IPSec only at times that it is needed.

Summary

Specific technical steps for implementing IPSec can be requested from DIS.With the above configuration the State of WA can move forward with its Windows 2000 project and accomplish a major milestone by April 30th. There are further steps which the state will need to continue working on to flush out the specifics. This foundation will facilitate further discussion and progress in the overall project.

Security Items to be Completed for the Forest Root

This section of the document identifies the essential security requirements for the root Windows 2000 domain to be brought up in production. This list was initially identified by Team3 and further approved by the Windows 2000 development group.

Group Policy Object

This section lists the Security Settings that are defined by default in the Default Domain Controller Policy GPO. This GPO is created when the first domain controller in the domain is installed via DCPromo. If this first domain controller is upgraded from a Windows NT 4.0 domain controller, then the values defined for the Windows NT 4.0 domain are used instead.
By default, these settings apply to all domain controllers in the domain. For a detailed description of each policy setting, refer to the Windows 2000 Server Resource Kit Online Help file for Group Policy, GP.CHM.

Key:

~~Strikethrough~~ = group decision to change default value

Policy	Default Value	Test Owner	Comment
Audit Policy			Check with auditors on these elements – see what their requirements are
Audit Account Logon events	~~No Auditing~~ Enable Auditing	John Ditto	Audit for both success and failure
Audit Account Management	~~No Auditing~~ Enable Auditing	John Ditto	Audit for both success and failure
Audit Policy Change	~~No Auditing~~ Enable Auditing	John Ditto	Audit for both success and failure
Audit System Events	~~No Auditing~~ Enable Auditing	John Ditto	Audit for both success and failure
User Rights Policy			
Access this computer from the network	Administrators, Authenticated Users, ~~Everyone~~	John Ditto	If the following groups were given this right prior to running DCPromo, then they are removed: Backup Operators, Guests, Guest, and Users. If a Windows NT 4.0 domain controller is upgraded as the first Windows 2000 domain

			controller using a slipstreamed setup of Windows 2000 + Service Pack 1, then the Authenticated Users group is automatically given this right.
Add workstations to the domain	~~Authenticated Users~~ Administrators	John Ditto	This User Right is for the support of legacy APIs. You can also allow users to create computer accounts by using this User Right. Authenticated Users can only create 10 computer accounts using this User Right.

These Group policy objects have been applied to the test root domain controllers.

Services

Microsoft Corporation is currently working on identifying these items and the document will be updated to reflect it.

Schema

The Default schema of the Windows 2000 root domain should not be changed until after April 30, 2001. Perform Forest prep after April 30, 2001 but before May 31, 2001 to get the forest ready for Exchange 2000 schema extensions. The schema will be frozen after May 31, 2001 until a schema change control policy is defined.

Lock down access

Identify up to 4 system administrators (including John Ditto of DIS) who will be Enterprise System Administrators for the root domain. Establish a process for Two Person Integrity (TPI) of enterprise administration accounts for the root to be in place before handing over to a root service provider. DIS document describing steps to connect agency domains first to the test domain and then to the production domain are described in the following sections.

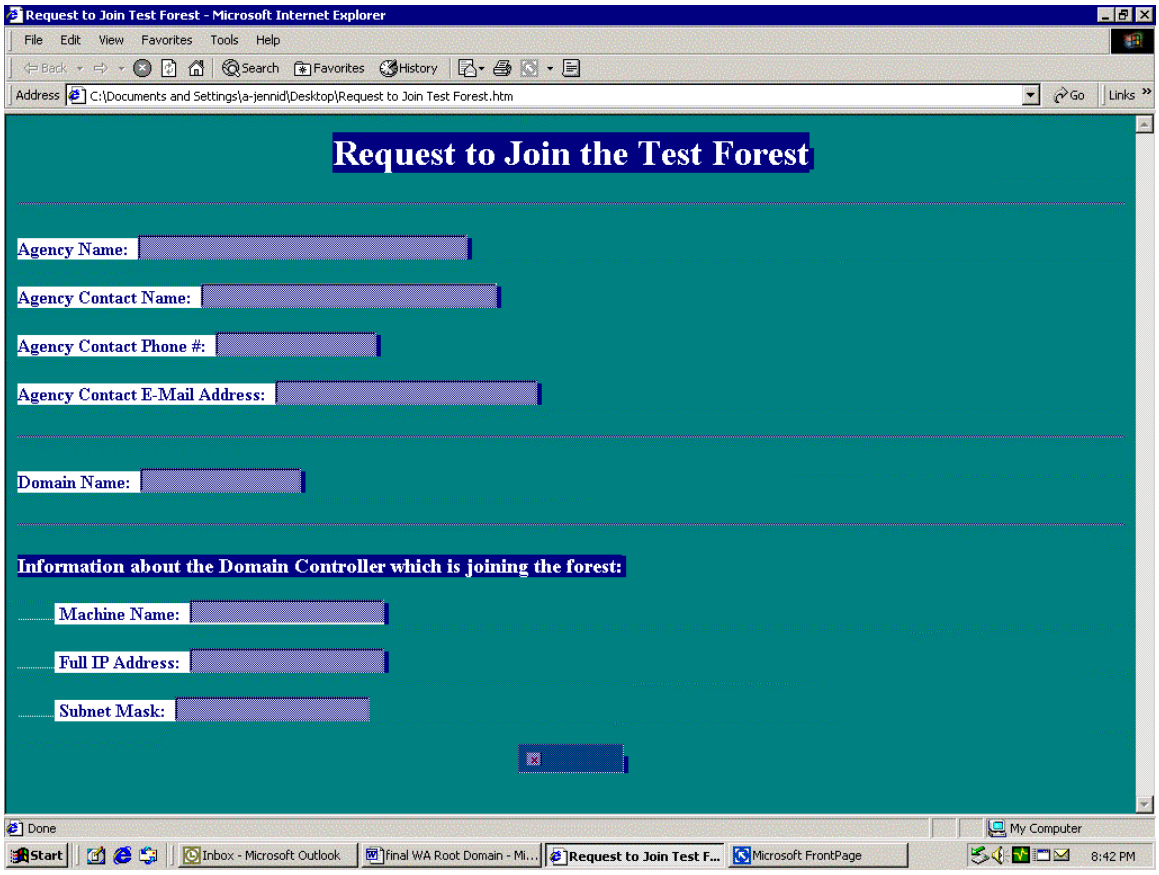
Compliance to State Security Policies (Digital Government)

The State Security Standard Password policy will be applied to the root domain before April 30, 2001. After April 30, 2001 it is recommend that State Auditors, Chuck Moore and Darlene Kossoff work with the Windows 2000 Development Group to ensure compliance and make recommendations for any modifications.

Physical Security Needs

DIS will provide a locked cabinet by April 30, 2001 to host the root Domain Controllers for the production root. DIS Security Office will have the key to the cabinet with a list of people who are allowed to have access. After April 30, 2001 the need for state wide advanced security technologies (IPSEC, PKI, CA, Biometrics, and Smartcard) and their impact should be considered.

Request to Join the Test Forest



Joining the Test Forest Instructions

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo
<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.TST. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.TST)	ECYLAN
<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest (*<MACHNAME>* is not referenced in this document. This value must have already been provided to DIS so that your machine can join this forest)	ECYTSTDC01

****

Step 1 is for Domains that are going to be joined into the Forest from behind a Firewall using IPSec.
If IPSec is not going to be implemented during Active Directory Installation, skip directly to Step 2.

****

Step: 1

Goal: Configure IPSec Policy to Join the Child Domain into the Forest.

Tasks	Detailed Steps
Configure Local Security Policy with for IPSec communication to install Active Directory from behind a Firewall.	1. Log on as Administrator. 2. Click the **Start** button, then select **Programs**, **Administrative Tools, Local Security Policy.** 3. Select **IP Security Policies on Local Machine**. 4. In the Results pane (right side), double click the **Server (Request Security) Policy**. 5. Select the **All IP Traffic Filter** and click **Edit**. 6. Select the **Authentication Methods** tab.

	7. Click **Add** to add a new authentication method. 8. In the **add authentication method** screen select the **Preshared Key** radial button and paste the preshared key given to you by DIS in the text window and click OK. 9. Repeat steps 5 – 8 for the **All ICMP Traffic** and **<Dynamic>** filters. All filters should now have 2 authentication methods, Kerberos as the default, and the Preshared Key as the secondary. 10. Click **OK** to close the **Server (Request Security) Properties** window. 11. In the **IP Security Local machine** results pane, right click the **Server (Request Security)** object, and select **Assign**.

****

After successfully installing Active Directory and rebooting, remove the PRESHARED Key from your IPSec Policy leaving only Kerberos.

****

Step: 2

Goal: Configure DNS suffix and point to the root domain server as the preferred DNS Server.

Tasks	Detailed Steps
Configure the DNS suffix for your computer. When prompted, restart the computer. Domain Suffix: ***<DOMAIN-NAME>***.*wa.tst* .	12. Log on as Administrator. 13. Open the **Properties** dialog box for My Computer. 14. In the **System Properties** dialog box, on the **Network Identification** tab, click **Properties**. 15. In the **Identification Changes** dialog box, click **More**. 16. In the **Primary DNS suffix of this computer** box, type ***<DOMAIN-NAME>***.*wa.tst* (e.g. **ecylan.wa.tst**., and then click **OK**. 17. Click **OK** to close the **Identification Changes** dialog box, and then click **OK** to close the **Network Identification** message box. 18. Click **OK** to close the **System Properties** dialog box, and then click **Yes** in the **System Settings Change** message box to restart your computer.
Configure the Internet	

Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS..	1. Log on as Administrator. 2. Right-click **My Network Places**, and then click **Properties**. 3. Right-click **Local Area Connection**, and then click **Properties**. 4. Click **Internet Protocol (TCP/IP)**, and the click **Properties** 5. In the **Preferred DNS Server** text box, you're your Server IP Address, and then click **OK**. 6. Click **OK** to close the **Local Area Connections Properties** box, and then close the **Network and Dial-up Connections** window.

Step: 3

Goal: Install and configure DNS.

Tasks	Detailed Steps
Install the Domain Name System (DNS) subcomponent of Networking Services. Copy the required files from the Windows 2000 Server compact disc.	1. Logon as Administrator for your Domain 2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Configure Your Server**. 3. Click **Networking** to expand and then click **DNS**. 4. Click **Set up DNS** on the right pane. 5. Insert the compact disc labeled Windows 2000 Advanced Server, and then click **OK**. 6. After the required files have been copied, click **Next**. 7. Expand **<MACHNAME>** 8. Right-click **<MACHNAME>** 9. Click **New Zone...** (New Zone Wizard is displayed) 10. Click **Next** 11. Click **Standard Primary** then click **Next** 12. Click **Forward Lookup Zone** then click **Next** 13. In the name field, enter **<DOMAIN-NAME>.WA.TST** (e.g. ecytst.wa.tst) 14. Click **Next**

	15. Click **Next** 16. Click **Finish** 17. Expand **Forward Lookup Zones** 18. Right-click **<DOMAIN-NAME>.WA.TST** 19. Click **Properties** 20. Change **Allow Dynamic Updates** to "**Yes**" 21. Click the **Forwarders** tab select the **Enable Forwarders** check box and add the IP Addresses of the Root DNS Servers as Forwarders. 22. Click **OK** 23. Close **DNS** 24. **Restart the computer**

Step: 4

Goal: Create a Windows 2000 domain by installing Active Directory.

Tasks	Detailed Steps
Start the Active Directory Installation wizard to create: A new domain controller for a new domain. A new domain tree. A new forest of domain trees.	1. Click **Start**, and then click **Run**. 2. In the **Run** box, type **dcpromo** and then click **OK**. 3. On the **Welcome to the Active Directory Installation Wizard** page, click **Next**. 4. On the **Domain Controller Type** page, ensure **Domain controller for a new domain** is selected, and then click **Next**. 5. On the **Create Tree or child Domain** page, select **Create a new child domain in an existing domain tree,** and then click **Next**. 6. On the **Network Credentials** page, enter the username of ***<JOIN-ID>*** (e.g. ECYPromo) and password and the domain of **wa.tst** and then click **Next**.

Complete the Active Directory installation process, providing the following information: Full DNS name of *wa.tst* .. Default locations for the database, log files, and shared system volume.	1. On the **Child Domain Installation** page, click Browse and select **wa.tst** to put **wa.tst** in the Parent Domain box and ***<DOMAIN-NAME>*** in the Child Domain box and then click **Next.** 2. On the **Netbios Domain Name** page, ensure ***<DOMAIN-NAME>*** is in the Domain Netbios name box and then click **Next**. 3. On the **Database and Log Locations** page, accept the default locations by clicking **Next** 4. On the **Shared System Volume** page, accept the default location by clicking **Next**. 5. On the **Permissions** page, select **Permissions compatible with pre-Windows 2000 servers**, and then click **Next**. 6. On the **Directory Services Restore Mode Administrator Password** page, in the **Password** and **Confirm password** boxes, type in the password and then click **Next**
Begin the Active Directory Installation/Replication process ..	On the **Summary** page, review the options you selected, and then click **Next**. 1. *The Active Directory Installation/Replication process begins.* 2. When the **Completing the Active Directory Installation Wizard** page appears, click **Finish**, and then restart your computer.

Step: 5

Goal: Enable GC on your domain's first Domain Controller.

Note – A GC should not host FSMO roles.

Tasks	Detailed Steps
Enable GC.	1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**. 2. In the console tree, expand **<DOMAIN-NAME>**, expand

	servers and then expand <**MACHNAME**>. 3. Right-click **NTDS settings** and then click **properties**. 4. Select the Global Catalog check box , and then click **OK**. 5. Close **Active Directory Sites and Services**. 6. Reboot Computer

Step: 6

Goal: Taking Ownership of Child Domain Site and Subnet.

Tasks	Detailed Steps
Taking Ownership of the Site and Subnet that was created by the Enterprise Administrators when pre-creating the Child Domain.	1. Open the **Active Directory Sites and Services** administration tool. 2. Expand the **Sites** object. 3. Right-click your Site name and select **Properties**. 4. Select the **Security** tab. 5. Select the **Advanced** button. 6. Select the **Owner** tab. 7. Select your **Domain Admins** group in the available list and select **OK**. 8. Expand the **Subnets** folder. 9. Right-click your IP Subnet and select **Properties**.

	10. Select the **Security** tab. 11. Select the **Advanced** button. 12. Select the **Owner** tab. 13. Select your **Domain Admins** group in the available list and select **OK**. 14. Close the **Active Directory Sites and Services** windows

Initial Setup by DIS for the FIRST New Agency (Domain) into the Test Forest

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a

collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo
<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.TST. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.TST)	ECYLAN
<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest	ECYDC01
<IP-ADDRESS>	IP Address of the Computer which is joining this Forest	
<NETWORK-IP>	Network IP address of the segment containing the agency's server which is joining the forest	198.234.56.0
<SUBNET-MASK>	Subnet mask for this segment containing the agency's server which is joining the forest	255.255.255.0
	Agency Contact Name	
	Agency Contact Phone Number	

****

Install Service Pack 1 before continuing with these instructions!

****

Step: 1
Goal: Pre-Stage all necessary OUs and Groups.

Tasks	Detailed Steps
Create OUs, and Groups necessary for Agency Domains to join into the Forest, and to have specific rights delegated to them	1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 2. Right-click the Domain object **WA.TST.** and select **NEW**.

to them.	then select **Organizational Unit.** Type **Promo Users** in the name box and select **OK.** 3. Right-click the Domain object **WA.TST,** and select **NEW**, then select **Organizational Unit.** Type **Service Delegation** in the name box and select **OK.** 4. Right-click the **Promo Users OU**, and select **New,** then select **Group.** 5. In the Group Name box type **L-S-Promo Users.** 6. Under the group scope options, select **Local**, and **Security** and press **OK.** 7. Right-click the **Service Delegation OU**, and select **New**, then select **Group.** 8. In the Group Name box type **U-S-WATST Forest DHCP Delegation.** 9. In the Description box type "**Universal Security Group for Delegating DHCP Authorization**". 10. Under the group scope options, select **Universal**, and **Security** and press **OK**. 11. Right-click the **Service Delegation OU**, and select **New**, then select **Group.** 12. In the Group Name box type **U-S-WATST Forest Sites and Services Delegation.** 13. In the Description box type "**Universal Security Group for Delegating Sites and Services control**". 14. Under the group scope options, select **Universal**, and **Security** and press **OK**.

Step: 2
Goal: Create a Child Zone for the Child Domain Server

Tasks	Detailed Steps
Create a Child Zone on the Child Domain Server	1. Logon as Administrator. 2. Start up **DNS Admin**. 3. Expand **Forward Lookup Zones** 4. Expand **WADC01TEST** 5. Right-click on **WA.TST** and select **New Host ....**

	6. Enter **<MACHNAME>** 7. Enter **<IP-ADDRESS>** in IP Address field 8. Click **Add Host** 9. Click **OK** and then click **Done** and verify that the computer was added in the right pane (may have to press F5 / Refresh) 10. Right-click on **WA.TST** and select **New Delegation..**. 11. Click **Next** 12. Enter **<DOMAIN-NAME>** 13. Click **Next** 14. Click **Add** 15. Click **Browse** 16. Browse to the entry just created and click **OK** 17. Click **OK** 18. Click **Next** 19. Click **Finish** 20. Close **DNS**

Step: 3
Goal: Create the user account that will be used to delegate to the child domain administrators to join the forest.

Tasks	Detailed Steps
Create the user account that will be used to delegate to create child domain	1. Logon as Administrator. 2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 3. Right-click the **Promo Users OU,** and click **New,** then select **User**. 4. Type the appropriate Join Forest ID ***<JOIN-ID>*** (e.g. ECYPromo) in **First name** and **User logon name**, and then click **Next**.

	5. Type appropriate password in **Password** and **Confirm password** box, and then click **Next**. 6. In the New Object user summary dialog box, click **Finish**. 7. Right click the New User Object and select **Properties.** Select the **Member Of** tab, click **Add**, and select the group named **L-S-Promo Users** and click **Add,** then click **OK.** 8. Close **Active Directory Users and Computers**.

Step: 4

Goal: Use ntdsutil to precreate child crossref object.

Tasks	Detailed Steps
Use NTDSUTIL to pre-create a child cross reference object.	1. Open a command prompt. 2. At the command prompt, type **NTDSUTIL**. 3. Type **Domain Management**. 4. Type **Connections**. 5. Type **Connect to Domain wa.tst**. 6. Type **quit**. 7. Type PRECREATE DC=***<DOMAIN-NAME>***,DC=WA,DC=TST ***<MACHNAME>***.***<DOMAIN-NAME>***.WA.TST e.g. **PRECREATE DC=ECY,DC=WA,DC=TST ECYTSTDC01.ECYLAN.WA.TST** *** **The PRECREATE command must be done in ALL UPPER CASE** *** 8. Type **quit**. 9. Type **quit**. 10. Close the command prompt window.

Step: 5

Goal: Create a new site for the new child domain.

In this exercise, you will create a new site for the new child domain.

Tasks	Detailed Steps

Create a new site	1. Click Start, point to Programs, point to Administrative Tools and then click to **Active Directory Sites and Services.** 2. Right click the **Sites** container and then click **New Site**. 3. Type ***<DOMAIN-NAME>*** for the new site in the Name box. 4. Click the Defaultipsitelink and then click OK. 5. Click OK.
Create a new subnet	1. Expand **Sites.** 2. Right click the **Subnets** container and then click **New Subnet** 3. Type in the ***<SEGMENT-IP>*** and ***<SUBNET-MASK>*** for this agency's subnet. 4. Click the new site created from the Select a site object for this subnet box, and then click OK. 5. Close all open windows.

Step: 6
Goal: Grant permission for members of the L-S-Promo Users to join a child domain to the root.

Tasks	Detailed Steps
Use ASDI Edit to grant permission for the child domain to join the root domain.	1. Click Start and then click Run. 2. In the **Run** box, type **mmc** and then click **OK**. 3. From the Console menu, click **Add/Remove Snap-in**… 4. Click **Add**. 5. Click **ADSI Edit** and then click **Add**. 6. Click **Close** to close the Add Standalone Snap-in dialog box. 7. Click **OK** to close Add/Remove Snap-in dialog box.

	8. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 9. Ensure Naming Context is **Domain NC** and click OK. 10. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 11. Pick **Configuration Container** from the Naming Context drop down box and then click **OK**. 12. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 13. Pick **Schema** from the Naming Context drop down box and then click **OK**.
Permissions for Configuration object	1. Expand **ADSI Edit**. 2. Expand **Configuration Container** and right-click **CN=Configuration object** and then click **Properties** 3. Click **Security** tab and then click **Add.** 4. Highlight **L-S-Promo Users** and then click **Add** and then click **OK**. 5. Click to allow **Read**, **Management Replication Topology**, **Replicating Directory Changes** and **Replication Synchronization** and then click **OK**.
Permissions for Schema object	1. Expand **Schema Container** and right-click **CN=Schema object** and then click **Properties**. 2. Click **Security** tab and then click **Add**. 3. Highlight **L-S-Promo Users** and then click **Add** and then click **OK**. 4. Click to allow **Read**, **Management Replication Topology**, **Replicating Directory Changes** and **Replication Synchronization** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	1. Expand **CN=Configuration** object**, Expand CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click Properties. 2. Click **Security** tab and then click **Add.** 3. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 4. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	1. Expand **CN=Configuration** object, Expand **CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click

	Properties. 2. Click **Security** tab and then click **Add**. 3. Highlight **Creator Owner** group and click **Add** and then click **OK**. 4. Click to allow **Full Control** and then click **OK**.
Permissions for Servers object	1. Expand **CN=*<DOMAIN-NAME>*** and then right-click **CN=Servers** and click **Properties**. 2. Click **Security** tab and then click **Add**. 3. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 4. Click to allow **Read** and **Create All Child Objects** and then click **OK.**
Permissions for ***<DOMAIN-NAME>*** object	1. Click **CN=Partitions** found underneath the Configuration object found in the Configuration container. 2. Right-click **CN=*<DOMAIN-NAME>*** and then click **Properties**. 3. Click **Security** tab and then click **Add**. 4. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 5. Click to allow **Full Control** and then click **OK**.
Permissions for System object	1. Expand **Domain NC** and expand **DC=wa,DC=tst**, and Right click **CN=System** object and then click **Properties**. 2. Click **Security** tab and then click **Add**. 3. Highlight **L-S-Promo Users** and click **Add** and then click **OK**. 4. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for System object	1. Right-click **CN=System** object and then click **Properties**. 2. Click **Security** tab and then click **Add**. 3. Highlight **Creator Owner** Group and click **Add** and then click **OK.** 4. Click to allow **Full Control** and then click **OK**. 5. Close all windows.

Step: 7
Goal: Delegate ability to authorize DHCP servers to the U-S-WATST Forest DHCP Delegation group.

Tasks	Detailed Steps
Delegate ability to authorize DHCP Servers to a non-enterprise adminsitrator	1. Open **Active Directory Sites and Services.** 2. On the **View** menu, click **Show Services Node** 3. In the console tree, expand **Services** and **click NetServices.** 4. On the **Action** Menu, click **Delegate Control**. The Delegation Control Wizard appears. 5. Click **Next** 6. Then, for **Users and Groups**, click **Add** 7. In select Users, Computers, or Groups locate and select **U-S-WATST Forest DHCP Delegation.** 8. Click **Add** and then click **OK** 9. For Delegate control of, select **This folder, existing objects in this folder, and creation of new objects in this folder** 10. Click **Next** 11. For **Permissions,** click **Full Control** and then click **Next**

Step: 8
Goal: Reset the Join ID password

Tasks	Detailed Steps
Reset the Join ID	1. Click Start**, point to Programs, point to Administrative Tools and then click Active Directory Users and Computers**

	2. **Expand WA.TST** 3. **Single-click on Promo Users** 4. **Right-click on <JOIN-ID> and select Reset Password...** 5. **Re-enter the Join ID's password in both field** 6. **Click OK** 7. **Close Active Directory Users and Computers**

Step: 9

Goal: Grant permission for the child domain administrators to create additional Sites and Subnets.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to Create new Sites, Subnets, and Site Links to child domain administrators.	1. Open **Active Directory Sites and Services.** 2. Right-Click the **SITES** object and select **Properties**, then select the **Security** tab. 3. Click Add, then select **Creator Owner** and click **OK**. 4. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 5. Click **Add**, then select **U-S-WATST Forest Sites and Services Delegation**, and click **OK**. 6. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**. 7. Expand the **SITES** object and Right-click the **SUBNETS** object and select **Properties**, then select the **Security** tab. 8. Click Add, then select **Creator Owner** and click **OK**. 9. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 10. Click **Add**, then select **U-S-WATST Forest Sites and Services Delegation**, and click **OK**. 11. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**. 12. Expand the **Inter-Site Transports** object and Right-click the **IP** object and select **Properties,** select the **Security** tab. 13. Click Add, then select **Creator Owner** and click **OK**.

	14. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 15. Click **Add**, then select **U-S-WATST Forest Sites and Services Delegation**, and click **OK**. 16. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**.

****

The following steps (10-11) cannot be performed until after the child domain has been joined to the forest successfully.

****

Step: 10

Goal: Add child domain's Domain Admins group to necessary Delegation groups

Note: For delegation to work properly, child domain must switch to Native Mode.

Tasks	Detailed Steps
Use Active Directory Users and Computers to join the child domain's Domain Admins group to the Universal groups that have delegated permissions in the forest for DHCP Authorization and Site management.	**1.** Open Active Directory **Users and Computers.** 2. **Expand** the **Service Delegation OU**. 3. Right-click the **U-S-WATST Forest DHCP Delegation** group and select **Properties** 4. Select the **Members** tab, then click **Add**. 5. in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 6. Click **OK** to close the **U-S-WATST Forest DHCP Delegation Properties** window. 7. Right-click the **U-S-WATST Forest Sites and Services Delegation** group and select **Properties** 8. Select the **Members** tab, then click **Add**. 9. in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**.

	then click **OK**. 10. Click **OK** to close the **U-S-WATST Forest Sites and Services Delegation Properties** window.

Step: 11

Goal: Give rights to child domain administrators to take control of their first Site and Subnet.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to the child domain administrators to take ownership of their first Site and Subnet.	**11.** Open Active Directory **Sites and Services.** 12. **Expand** the Sites object. 13. Right-click the child domain's site that was created by the Enterprise Administrators before the child domain was joined and select **Properties**. 14. Select the **Security** tab, then click the **Advanced** button. 15. Click **Add,** and in the **Look in:** box select the child domain. 16. Select the child domain's **Domain Admins** group and click **OK**. 17. Under the **Allow** column select the **Read Permissions**, **Modify Permissions**, and **Modify Owner** check boxes and click **OK**. 18. Repeat steps 1 to 7 for the child domain's **Subnet** object.

Initial Setup by DIS for a New Agency (Domain), Other than the FIRST New Agency (Domain) into the Test Forest.

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo
<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.TST. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.TST)	ECYLAN
<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest	ECYDC01
<IP-ADDRESS>	IP Address of the Computer which is joining this Forest	
<NETWORK-IP>	Network IP address of the segment containing the agency's server which is joining the forest	198.234.56.0
<SUBNET-MASK>	Subnet mask for this segment containing the agency's server which is joining the forest	255.255.255.0
	Agency Contact Name	
	Agency Contact Phone Number	

Step: 1
Goal: Create a Child Zone for the Child Domain Server

Tasks	Detailed Steps
Create a Child Zone on the Child Domain Server	1. Logon as Administrator. 2. Start up **DNS Admin**. 3. Expand **Forward Lookup Zones** 4. Expand **WADC01TEST** 5. Right-click on **WA.TST** and select **New Host ....** 6. Enter **<MACHNAME>** 7. Enter **<IP-ADDRESS>** in IP Address field

	8. Click **Add Host** 9. Click **OK** and then click **Done** and verify that the computer was added in the right pane (may have to press F5 / Refresh) 10. Right-click on **WA.TST** and select **New Delegation..**. 11. Click **Next** 12. Enter **<DOMAIN-NAME>** 13. Click **Next** 14. Click **Add** 15. Click **Browse** 16. Browse to the entry just created and click **OK** 17. Click **OK** 18. Click **Next** 19. Click **Finish** 20. Close **DNS**

Step: 2
Goal: Create the user account that will be used to delegate to the child domain administrators to join the forest.

Tasks	Detailed Steps
Create the user account that will be used to delegate to create child domain	9. Logon as Administrator. 10. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 11. Right-click the **Promo Users OU,** and click **New,** then select **User**. 12. Type the appropriate Join Forest ID ***<JOIN-ID>*** (e.g. ECYPromo) in **First name** and **User logon name**, and then click **Next**. 13. Type appropriate password in **Password** and **Confirm**

	password box, and then click **Next**. 14. In the New Object user summary dialog box, click **Finish**. 15. Right click the New User Object and select **Properties.** Select the **Member Of** tab, click **Add**, and select the group named **L-S-Promo Users** and click **Add,** then click **OK.** 16. Close **Active Directory Users and Computers**.

Step: 3

Goal: Use ntdsutil to precreate child crossref object.

Tasks	Detailed Steps
Use NTDSUTIL to pre-create a child cross reference object.	11. Open a command prompt. 12. At the command prompt, type **NTDSUTIL**. 13. Type **Domain Management**. 14. Type **Connections**. 15. Type **Connect to Domain wa.tst**. 16. Type **quit**. 17. Type PRECREATE DC=***<DOMAIN-NAME>***,DC=WA,DC=TST ***<MACHNAME>***.***<DOMAIN-NAME>***.WA.TST e.g. **PRECREATE DC=ECY,DC=WA,DC=TST ECYTSTDC01.ECYLAN.WA.TST** ** **The PRECREATE command must be done in ALL UPPER CASE** ** 18. Type **quit**. 19. Type **quit**. 20. Close the command prompt window.

Step: 4

Goal: Create a new site for the new child domain.

In this exercise, you will create a new site for the new child domain.

Tasks	Detailed Steps
Create a new site	6. Click Start, point to Programs, point to Administrative

	Tools and then click to **Active Directory Sites and Services.** 7. Right click the **Sites** container and then click **New Site**. 8. Type ***<DOMAIN-NAME>*** for the new site in the Name box. 9. Click the Defaultipsitelink and then click OK. 10. Click OK.
Create a new subnet	6. Expand **Sites.** 7. Right click the **Subnets** container and then click **New Subnet** 8. Type in the ***<SEGMENT-IP>*** and ***<SUBNET-MASK>*** for this agency's subnet. 9. Click the new site created from the Select a site object for this subnet box, and then click OK. 10. Close all open windows.

Step: 5
Goal: Grant necessary permissions for child domain administrators to join a child domain to the root.

Tasks	Detailed Steps
Using ADSI Edit, give necessary permissions for joining a child domain.	1. Click Start and then click Run. 2. In the **Run** box, type **mmc** and then click **OK**. 3. From the Console menu, click **Add/Remove Snap-in**… 4. Click **Add**. 5. Click **ADSI Edit** and then click **Add**. 6. Click **Close** to close the Add Standalone Snap-in dialog box. 7. Click **OK** to close Add/Remove Snap-in dialog box. 8. From the Console dialog box, right-click **ADSI Edit** and

	click **Connect to**…. 9. Ensure Naming Context is **Domain NC** and click OK. 10. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 11. Pick **Configuration Container** from the Naming Context drop down box and then click **OK**. 12. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 13. Pick **Schema** from the Naming Context drop down box and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	5. Expand **CN=Configuration** object**, Expand CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click Properties. 6. Click **Security** tab and then click **Add.** 7. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 8. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	5. Expand **CN=Configuration** object, Expand **CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click **Properties**. 6. Click **Security** tab and then click **Add**. 7. Highlight **Creator Owner** group and click **Add** and then click **OK**. 8. Click to allow **Full Control** and then click **OK**.
Permissions for Servers object	5. Expand **CN=*<DOMAIN-NAME>*** and then right-click **CN=Servers** and click **Properties**. 6. Click **Security** tab and then click **Add**. 7. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 8. Click to allow **Read** and **Create All Child Objects** and then click **OK.**
Permissions for ***<DOMAIN-NAME>*** object	6. Click **CN=Partitions** found underneath the Configuration object found in the Configuration container. 7. Right-click **CN=*<DOMAIN-NAME>*** and then click **Properties**.

	8. Click **Security** tab and then click **Add**. 9. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 10. Click to allow **Full Control** and then click **OK**.

Step: 6
Goal: Reset the Join ID password

Tasks	Detailed Steps
Reset the Join ID	**8. Click Start, point to Programs, point to Administrative Tools and then click Active Directory Users and Computers** **9. Expand WA.TST** **10. Single-click on Promo Users** **11. Right-click on <JOIN-ID> and select Reset Password...** **12. Re-enter the Join ID's password in both field** **13. Click OK** 14. **Close Active Directory Users and Computers**

****

The following steps (7-8) cannot be performed until after the child domain has been joined to the forest successfully.

****

Step: 7
Goal: Add child domain's Domain Admins group to necessary Delegation groups
Note: For delegation to work properly, child domain must switch to Native Mode.

Tasks	Detailed Steps
Use Active Directory Users and Computers to join the child domain's Domain Admins group	**3** Open Active Directory **Users and Computers.** **4** **Expand** the **Service Delegation OU**.

to the Universal groups that have delegated permissions in the forest for DHCP Authorization and Site management.	**5** Right-click the **U-S-WATST Forest DHCP Delegation** group and select **Properties** 6 Select the **Members** tab, then click **Add**. 7 in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 8 Click **OK** to close the **U-S-WATST Forest DHCP Delegation Properties** window. 9 Right-click the **U-S-WATST Forest Sites and Services Delegation** group and select **Properties** 10 Select the **Members** tab, then click **Add**. 11 in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 12 Click **OK** to close the **U-S-WATST Forest Sites and Services Delegation Properties** window.

Step: 8
Goal: Give rights to child domain administrators to take control of their first Site and Subnet.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to the child domain administrators to take ownership of their first Site and Subnet.	**21.** Open Active Directory **Sites and Services.** 22. **Expand** the Sites object. 23. Right-click the child domain's site that was created by the Enterprise Administrators before the child domain was joined and select **Properties**. 24. Select the **Security** tab, then click the **Advanced** button. 25. Click **Add,** and in the **Look in:** box select the child domain. 26. Select the child domain's **Domain Admins** group and click **OK**. 27. Under the **Allow** column select the **Read Permissions**, **Modifv Permissions**. and **Modifv Owner** check boxes

	and click **OK**. 28. Repeat steps 1 to 7 for the child domain's **Subnet** object.

Initial Setup by DIS for the FIRST New Agency (Domain) into the Production Forest

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo
<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.LCL. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.LCL)	ECYLAN

<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest	ECYDC01
<IP-ADDRESS>	IP Address of the Computer which is joining this Forest	
<NETWORK-IP>	Network IP address of the segment containing the agency's server which is joining the forest	198.234.56.0
<SUBNET-MASK>	Subnet mask for this segment containing the agency's server which is joining the forest	255.255.255.0
	Agency Contact Name	
	Agency Contact Phone Number	

****

Install Service Pack 1 before continuing with these instructions!

****

Step: 1
Goal: Pre-Stage all necessary OUs and Groups.

Tasks	Detailed Steps
Create OUs, and Groups necessary for Agency Domains to join into the Forest, and to have specific rights delegated to them.	15. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 16. Right-click the Domain object **WA.LCL,** and select **NEW**, then select **Organizational Unit.** Type **Promo Users** in the name box and select **OK.** 17. Right-click the Domain object **WA.LCL,** and select **NEW**, then select **Organizational Unit.** Type **Service Delegation** in the name box and select **OK.** 18. Right-click the **Promo Users OU**, and select **New,** then select **Group.** 19. In the Group Name box type **L-S-Promo Users.** 20. Under the group scope options, select **Local**, and **Security** and press **OK.** 21. Right-click the **Service Delegation OU**, and select **New**,

	then select **Group.** 22. In the Group Name box type **U-S-WALCL Forest DHCP Delegation.** 23. In the Description box type "**Universal Security Group for Delegating DHCP Authorization**". 24. Under the group scope options, select **Universal**, and **Security** and press **OK**. 25. Right-click the **Service Delegation OU**, and select **New**, then select **Group.** 26. In the Group Name box type **U-S-WALCL Forest Sites and Services Delegation.** 27. In the Description box type "**Universal Security Group for Delegating Sites and Services control**". 28. Under the group scope options, select **Universal**, and **Security** and press **OK**.

Step: 2
Goal: Create a Child Zone for the Child Domain Server

Tasks	Detailed Steps
Create a Child Zone on the Child Domain Server	21. Logon as Administrator. 22. Start up **DNS Admin**. 23. Expand **Forward Lookup Zones** 24. Expand **WADC01TEST** 25. Right-click on **WA.LCL** and select **New Host ....** 26. Enter **<MACHNAME>** 27. Enter **<IP-ADDRESS>** in IP Address field 28. Click **Add Host** 29. Click **OK** and then click **Done** and verify that the computer was added in the right pane (may have to press F5 / Refresh) 30. Right-click on **WA.LCL** and select **New Delegation..**. 31. Click **Next** 32. Enter **<DOMAIN-NAME>**

	33. Click **Next** 34. Click **Add** 35. Click **Browse** 36. Browse to the entry just created and click **OK** 37. Click **OK** 38. Click **Next** 39. Click **Finish** 40. Close **DNS**

Step: 3
Goal: Create the user account that will be used to delegate to the child domain administrators to join the forest.

Tasks	Detailed Steps
Create the user account that will be used to delegate to create child domain	17. Logon as Administrator. 18. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 19. Right-click the **Promo Users OU,** and click **New,** then select **User**. 20. Type the appropriate Join Forest ID ***<JOIN-ID>*** (e.g. ECYPromo) in **First name** and **User logon name**, and then click **Next**. 21. Type appropriate password in **Password** and **Confirm password** box, and then click **Next**. 22. In the New Object user summary dialog box, click **Finish**. 23. Right click the New User Object and select **Properties.** Select the **Member Of** tab, click **Add**, and select the group named **L-S-Promo Users** and click **Add,** then click **OK.** 24. Close **Active Directory Users and Computers**.

Step: 4

Goal: Use ntdsutil to precreate child crossref object.

Tasks	Detailed Steps
Use NTDSUTIL to pre-create a child cross reference object.	21. Open a command prompt. 22. At the command prompt, type **NTDSUTIL**. 23. Type **Domain Management**. 24. Type **Connections**. 25. Type **Connect to Domain WA.LCL**. 26. Type **quit**. 27. Type PRECREATE DC=***<DOMAIN-NAME>***,DC=WA,DC=TST ***<MACHNAME>***.***<DOMAIN-NAME>***.WA.LCL e.g. **PRECREATE DC=ECY,DC=WA,DC=TST ECYTSTDC01.ECYLAN.WA.LCL** ** **The PRECREATE command must be done in ALL UPPER CASE** ** 28. Type **quit**. 29. Type **quit**. 30. Close the command prompt window.

Step: 5

Goal: Create a new site for the new child domain.

In this exercise, you will create a new site for the new child domain.

Tasks	Detailed Steps
Create a new site	11. Click Start, point to Programs, point to Administrative Tools and then click to **Active Directory Sites and Services.** 12. Right click the **Sites** container and then click **New Site**. 13. Type ***<DOMAIN-NAME>*** for the new site in the Name box. 14. Click the Defaultipsitelink and then click OK. 15. Click OK.

Create a new subnet	11. Expand **Sites.** 12. Right click the **Subnets** container and then click **New Subnet** 13. Type in the ***<SEGMENT-IP>*** and ***<SUBNET-MASK>*** for this agency's subnet. 14. Click the new site created from the Select a site object for this subnet box, and then click OK. 15. Close all open windows.

Step: 6

Goal: Grant permission for members of the L-S-Promo Users to join a child domain to the root.

Tasks	Detailed Steps
Use ASDI Edit to grant permission for the child domain to join the root domain.	14. Click Start and then click Run. 15. In the **Run** box, type **mmc** and then click **OK**. 16. From the Console menu, click **Add/Remove Snap-in**… 17. Click **Add**. 18. Click **ADSI Edit** and then click **Add**. 19. Click **Close** to close the Add Standalone Snap-in dialog box. 20. Click **OK** to close Add/Remove Snap-in dialog box. 21. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 22. Ensure Naming Context is **Domain NC** and click OK. 23. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 24. Pick **Configuration Container** from the Naming Context drop down box and then click **OK**. 25. From the Console dialog box, right-click **ADSI Edit** and

	click **Connect to**…. 26. Pick **Schema** from the Naming Context drop down box and then click **OK**.
Permissions for Configuration object	6. Expand **ADSI Edit**. 7. Expand **Configuration Container** and right-click **CN=Configuration object** and then click **Properties** 8. Click **Security** tab and then click **Add.** 9. Highlight **L-S-Promo Users** and then click **Add** and then click **OK**. 10. Click to allow **Read**, **Management Replication Topology**, **Replicating Directory Changes** and **Replication Synchronization** and then click **OK**.
Permissions for Schema object	5. Expand **Schema Container** and right-click **CN=Schema object** and then click **Properties**. 6. Click **Security** tab and then click **Add**. 7. Highlight **L-S-Promo Users** and then click **Add** and then click **OK**. 8. Click to allow **Read**, **Management Replication Topology**, **Replicating Directory Changes** and **Replication Synchronization** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	9. Expand **CN=Configuration** object**, Expand CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click Properties. 10. Click **Security** tab and then click **Add.** 11. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 12. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	9. Expand **CN=Configuration** object, Expand **CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click **Properties**. 10. Click **Security** tab and then click **Add**. 11. Highlight **Creator Owner** group and click **Add** and then click **OK**. 12. Click to allow **Full Control** and then click **OK**.
Permissions for Servers object	9. Expand **CN=*<DOMAIN-NAME>*** and then right-click **CN=Servers** and click **Properties**.

	10. Click **Security** tab and then click **Add**. 11. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 12. Click to allow **Read** and **Create All Child Objects** and then click **OK.**
Permissions for ***<DOMAIN-NAME>*** object	11. Click **CN=Partitions** found underneath the Configuration object found in the Configuration container. 12. Right-click **CN=*<DOMAIN-NAME>*** and then click **Properties**. 13. Click **Security** tab and then click **Add**. 14. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 15. Click to allow **Full Control** and then click **OK**.
Permissions for System object	5. Expand **Domain NC** and expand **DC=wa,DC=tst**, and Right click **CN=System** object and then click **Properties**. 6. Click **Security** tab and then click **Add**. 7. Highlight **L-S-Promo Users** and click **Add** and then click **OK**. 8. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for System object	6. Right-click **CN=System** object and then click **Properties**. 7. Click **Security** tab and then click **Add**. 8. Highlight **Creator Owner** Group and click **Add** and then click **OK.** 9. Click to allow **Full Control** and then click **OK**. 10. Close all windows.

Step: 7
Goal: Delegate ability to authorize DHCP servers to the U-S-WALCL Forest DHCP Delegation group.

Tasks	Detailed Steps
Delegate ability to authorize DHCP Servers to a non-enterprise adminsitrator	**12.** Open **Active Directory Sites and Services.** 13. On the **View** menu, click **Show Services Node** 14. In the console tree, expand **Services** and **click**

	NetServices. 15. On the **Action** Menu, click **Delegate Control**. The Delegation Control Wizard appears. 16. Click **Next** 17. Then, for **Users and Groups**, click **Add** 18. In select Users, Computers, or Groups locate and select **U-S-WALCL Forest DHCP Delegation.** 19. Click **Add** and then click **OK** 20. For Delegate control of, select **This folder, existing objects in this folder, and creation of new objects in this folder** 21. Click **Next** 22. For **Permissions,** click **Full Control** and then click **Next**

Step: 8
Goal: Reset the Join ID password

Tasks	Detailed Steps
Reset the Join ID	**15.** Click Start**, point to Programs, point to Administrative Tools and then click Active Directory Users and Computers** **16. Expand WA.LCL** **17. Single-click on Promo Users** **18. Right-click on <JOIN-ID> and select Reset Password...** **19. Re-enter the Join ID's password in both field** **20. Click OK** 21. **Close Active Directory Users and Computers**

Step: 9

Goal: Grant permission for the child domain administrators to create additional Sites and Subnets.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to Create new Sites, Subnets, and Site Links to child domain administrators.	17. Open **Active Directory Sites and Services.** 18. Right-Click the **SITES** object and select **Properties**, then select the **Security** tab. 19. Click Add, then select **Creator Owner** and click **OK**. 20. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 21. Click **Add**, then select **U-S-WALCL Forest Sites and Services Delegation**, and click **OK**. 22. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**. 23. Expand the **SITES** object and Right-click the **SUBNETS** object and select **Properties**, then select the **Security** tab. 24. Click Add, then select **Creator Owner** and click **OK**. 25. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 26. Click **Add**, then select **U-S-WALCL Forest Sites and Services Delegation**, and click **OK**. 27. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**. 28. Expand the **Inter-Site Transports** object and Right-click the **IP** object and select **Properties,** select the **Security** tab. 29. Click Add, then select **Creator Owner** and click **OK**. 30. Highlight **Creator Owner** and select the **Allow**, **Full Control** check box and click **Apply.** 31. Click **Add**, then select **U-S-WALCL Forest Sites and Services Delegation**, and click **OK**. 32. Highlight **U-S-Sites and Services** and select the **Allow**, **Create All Child Objects** check box and click **OK**.

****

The following steps (10-11) cannot be performed until after the child domain has been joined to the forest successfully.

****

Step: 10

Goal: Add child domain's Domain Admins group to necessary Delegation groups

Note: For delegation to work properly, child domain must switch to Native Mode.

Tasks	Detailed Steps
Use Active Directory Users and Computers to join the child domain's Domain Admins group to the Universal groups that have delegated permissions in the forest for DHCP Authorization and Site management.	**19.** Open Active Directory **Users and Computers.** 20. **Expand** the **Service Delegation OU**. 21. Right-click the **U-S-WALCL Forest DHCP Delegation** group and select **Properties** 22. Select the **Members** tab, then click **Add**. 23. in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 24. Click **OK** to close the **U-S-WALCL Forest DHCP Delegation Properties** window. 25. Right-click the **U-S-WALCL Forest Sites and Services Delegation** group and select **Properties** 26. Select the **Members** tab, then click **Add**. 27. in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 28. Click **OK** to close the **U-S-WALCL Forest Sites and Services Delegation Properties** window.

Step: 11

Goal: Give rights to child domain administrators to take control of their first Site and Subnet.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to the child domain administrators to take ownership of their first Site and Subnet.	**29.** Open Active Directory **Sites and Services.** 30. **Expand** the Sites object. 31. Right-click the child domain's site that was created by the Enterprise Administrators before the child domain was joined and select **Properties**. 32. Select the **Security** tab, then click the **Advanced** button. 33. Click **Add,** and in the **Look in:** box select the child domain. 34. Select the child domain's **Domain Admins** group and click **OK**. 35. Under the **Allow** column select the **Read Permissions**, **Modify Permissions**, and **Modify Owner** check boxes and click **OK**. 36. Repeat steps 1 to 7 for the child domain's **Subnet** object.

Initial Setup by DIS for a New Agency (Domain), Other than the FIRST New Agency (Domain) into the Production Forest.

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo
<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.LCL. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.LCL)	ECYLAN
<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest	ECYDC01
<IP-ADDRESS>	IP Address of the Computer which is joining this Forest	
<NETWORK-IP>	Network IP address of the segment containing the agency's server which is joining the forest	198.234.56.0
<SUBNET-MASK>	Subnet mask for this segment containing the agency's server which is joining the forest	255.255.255.0
	Agency Contact Name	
	Agency Contact Phone Number	

Step: 1
Goal: Create a Child Zone for the Child Domain Server

Tasks	Detailed Steps
Create a Child Zone on the Child Domain Server	29. Logon as Administrator. 30. Start up **DNS Admin**. 31. Expand **Forward Lookup Zones** 32. Expand **WADC01TEST** 33. Right-click on **WA.LCL** and select **New Host ....** 34. Enter **<MACHNAME>** 35. Enter **<IP-ADDRESS>** in IP Address field

	36. Click **Add Host** 37. Click **OK** and then click **Done** and verify that the computer was added in the right pane (may have to press F5 / Refresh) 38. Right-click on **WA.LCL** and select **New Delegation..**. 39. Click **Next** 40. Enter **<DOMAIN-NAME>** 41. Click **Next** 42. Click **Add** 43. Click **Browse** 44. Browse to the entry just created and click **OK** 45. Click **OK** 46. Click **Next** 47. Click **Finish** 48. Close **DNS**

Step: 2
Goal: Create the user account that will be used to delegate to the child domain administrators to join the forest.

Tasks	Detailed Steps
Create the user account that will be used to delegate to create child domain	25. Logon as Administrator. 26. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. 27. Right-click the **Promo Users OU,** and click **New,** then select **User**. 28. Type the appropriate Join Forest ID ***<JOIN-ID>*** (e.g. ECYPromo) in **First name** and **User logon name**, and then click **Next**. 29. Type appropriate password in **Password** and **Confirm**

	password box, and then click **Next**. 30. In the New Object user summary dialog box, click **Finish**. 31. Right click the New User Object and select **Properties.** Select the **Member Of** tab, click **Add**, and select the group named **L-S-Promo Users** and click **Add,** then click **OK.** 32. Close **Active Directory Users and Computers**.

Step: 3

Goal: Use ntdsutil to precreate child crossref object.

Tasks	Detailed Steps
Use NTDSUTIL to pre-create a child cross reference object.	31. Open a command prompt. 32. At the command prompt, type **NTDSUTIL**. 33. Type **Domain Management**. 34. Type **Connections**. 35. Type **Connect to Domain WA.LCL**. 36. Type **quit**. 37. Type PRECREATE DC=***<DOMAIN-NAME>***,DC=WA,DC=TST ***<MACHNAME>***.***<DOMAIN-NAME>***.WA.LCL e.g. **PRECREATE DC=ECY,DC=WA,DC=TST ECYTSTDC01.ECYLAN.WA.LCL** *** **The PRECREATE command must be done in ALL UPPER CASE** *** 38. Type **quit**. 39. Type **quit**. 40. Close the command prompt window.

Step: 4

Goal: Create a new site for the new child domain.

In this exercise, you will create a new site for the new child domain.

Tasks	Detailed Steps
Create a new site	16. Click Start, point to Programs, point to Administrative

	Tools and then click to **Active Directory Sites and Services.** 17. Right click the **Sites** container and then click **New Site**. 18. Type ***<DOMAIN-NAME>*** for the new site in the Name box. 19. Click the Defaultipsitelink and then click OK. 20. Click OK.
Create a new subnet	16. Expand **Sites.** 17. Right click the **Subnets** container and then click **New Subnet** 18. Type in the ***<SEGMENT-IP>*** and ***<SUBNET-MASK>*** for this agency's subnet. 19. Click the new site created from the Select a site object for this subnet box, and then click OK. 20. Close all open windows.

Step: 5
Goal: Grant necessary permissions for child domain administrators to join a child domain to the root.

Tasks	Detailed Steps
Using ADSI Edit, give necessary permissions for joining a child domain.	14. Click Start and then click Run. 15. In the **Run** box, type **mmc** and then click **OK**. 16. From the Console menu, click **Add/Remove Snap-in**… 17. Click **Add**. 18. Click **ADSI Edit** and then click **Add**. 19. Click **Close** to close the Add Standalone Snap-in dialog box. 20. Click **OK** to close Add/Remove Snap-in dialog box. 21. From the Console dialog box, right-click **ADSI Edit** and

	click **Connect to**…. 22. Ensure Naming Context is **Domain NC** and click OK. 23. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 24. Pick **Configuration Container** from the Naming Context drop down box and then click **OK**. 25. From the Console dialog box, right-click **ADSI Edit** and click **Connect to**…. 26. Pick **Schema** from the Naming Context drop down box and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	13. Expand **CN=Configuration** object**, Expand CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click Properties. 14. Click **Security** tab and then click **Add.** 15. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 16. Click to allow **Read** and **Create All Child Objects** and then click **OK**.
Permissions for ***<DOMAIN-NAME>*** object	13. Expand **CN=Configuration** object, Expand **CN=Sites** and then right-click **CN=*<DOMAIN-NAME>*** object and click **Properties**. 14. Click **Security** tab and then click **Add**. 15. Highlight **Creator Owner** group and click **Add** and then click **OK**. 16. Click to allow **Full Control** and then click **OK**.
Permissions for Servers object	13. Expand **CN=*<DOMAIN-NAME>*** and then right-click **CN=Servers** and click **Properties**. 14. Click **Security** tab and then click **Add**. 15. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 16. Click to allow **Read** and **Create All Child Objects** and then click **OK.**
Permissions for ***<DOMAIN-NAME>*** object	16. Click **CN=Partitions** found underneath the Configuration object found in the Configuration container. 17. Right-click **CN=*<DOMAIN-NAME>*** and then click **Properties**.

	18. Click **Security** tab and then click **Add**. 19. Highlight ***<Join-ID>*** and click **Add** and then click **OK**. 20. Click to allow **Full Control** and then click **OK**.

Step: 6
Goal: Reset the Join ID password

Tasks	Detailed Steps
Reset the Join ID	**22. Click Start, point to Programs, point to Administrative Tools and then click Active Directory Users and Computers** **23. Expand WA.LCL** **24. Single-click on Promo Users** **25. Right-click on <JOIN-ID> and select Reset Password...** **26. Re-enter the Join ID's password in both field** **27. Click OK** **28. Close Active Directory Users and Computers**

****

The following steps (7-8) cannot be performed until after the child domain has been joined to the forest successfully.

****

Step: 7
Goal: Add child domain's Domain Admins group to necessary Delegation groups
Note: For delegation to work properly, child domain must switch to Native Mode.

Tasks	Detailed Steps
Use Active Directory Users and Computers to join the child domain's Domain Admins group	**3** Open Active Directory **Users and Computers.** **4** **Expand** the **Service Delegation OU**.

to the Universal groups that have delegated permissions in the forest for DHCP Authorization and Site management.	**5** Right-click the **U-S-WALCL Forest DHCP Delegation** group and select **Properties** 6 Select the **Members** tab, then click **Add**. 7 in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 8 Click **OK** to close the **U-S-WALCL Forest DHCP Delegation Properties** window. 9 Right-click the **U-S-WALCL Forest Sites and Services Delegation** group and select **Properties** 10 Select the **Members** tab, then click **Add**. 11 in the **Look in:** box, select the child domain, then select the **Domain Admins** group for that domain and click **Add**, then click **OK**. 12 Click **OK** to close the **U-S-WALCL Forest Sites and Services Delegation Properties** window.

Step: 8
Goal: Give rights to child domain administrators to take control of their first Site and Subnet.

Tasks	Detailed Steps
Use Active Directory Sites and Services to Delegate the right to the child domain administrators to take ownership of their first Site and Subnet.	**49.** Open Active Directory **Sites and Services.** 50. **Expand** the Sites object. 51. Right-click the child domain's site that was created by the Enterprise Administrators before the child domain was joined and select **Properties**. 52. Select the **Security** tab, then click the **Advanced** button. 53. Click **Add,** and in the **Look in:** box select the child domain. 54. Select the child domain's **Domain Admins** group and click **OK**. 55. Under the **Allow** column select the **Read Permissions**, **Modifv Permissions**. and **Modifv Owner** check boxes

	and click **OK**. 56. Repeat steps 1 to 7 for the child domain's **Subnet** object.

Joining the Production Forest Instructions

This document is written with the following three variable names which must be resolved to real names before these instructions can be followed. Their real names are based upon a collaborative agreement between DIS and the agency which is going to Join this Forest. These three variable names and their meanings are as follows:

Variable Name	Meaning	Example
<Join-ID>	Admin Userid provided by DIS which has sufficient permissions for joining this forest	ECYPromo

<DOMAIN-NAME>	Windows 2000 Domain Name. This is the subdomain name immediately to the left of WA.LCL. Examples of this would be ECY or ECYLAN (as in ECYLAN.WA.LCL)	ECYLAN
<MACHNAME>	Computer Name of the Domain Controller which is joining this Forest (***<MACHNAME>*** is not referenced in this document. This value must have already been provided to DIS so that your machine can join this forest)	ECYTSTDC01

Note: If for some reason as an Agency experiences a failed DCPROMO (in Step 2), please contact DIS before trying again. They will ensure that the root is cleaned properly to allow a complete and clean connection to the agency.

****

Step 1 is for Domains that are going to be joined into the Forest from behind a Firewall using IPSec.
If IPSec is not going to be implemented during Active Directory Installation, skip directly to Step 2.

****

Step: 1

Goal: Configure IPSec Policy to Join the Child Domain into the Forest.

Tasks	Detailed Steps
Configure Local Security Policy with for IPSec communication to install Active Directory from behind a Firewall.	19. Log on as Administrator. 20. Click the **Start** button, then select **Programs**, **Administrative Tools, Local Security Policy.** 21. Select **IP Security Policies on Local Machine**. 22. In the Results pane (right side), double click the **Server (Request Security) Policy**. 23. Select the **All IP Traffic Filter** and click **Edit**. 24. Select the **Authentication Methods** tab. 25. Click **Add** to add a new authentication method. 26. In the **add authentication method** screen select the **Preshared Key** radial button and paste the preshared key given to you by DIS in the text window and click OK. 27. Repeat steps 5 – 8 for the **All ICMP Traffic** and **<Dynamic>** filters. All filters should now have 2 authentication methods. Kerberos as the

	default, and the Preshared Key as the secondary. 28. Click **OK** to close the **Server (Request Security) Properties** window. 29. In the **IP Security Local machine** results pane, right click the **Server (Request Security)** object, and select **Assign**.

****

After successfully installing Active Directory and rebooting, remove the PRESHARED Key from your IPSec Policy leaving only Kerberos.

****

Step: 2

Goal: Configure DNS suffix and point to the root domain server as the preferred DNS Server.

Tasks	Detailed Steps
Configure the DNS suffix for your computer. When prompted, restart the computer. Domain Suffix: ***<DOMAIN-NAME>***.*WA.LCL* .	30. Log on as Administrator. 31. Open the **Properties** dialog box for My Computer. 32. In the **System Properties** dialog box, on the **Network Identification** tab, click **Properties**. 33. In the **Identification Changes** dialog box, click **More**. 34. In the **Primary DNS suffix of this computer** box, type ***<DOMAIN-NAME>***.*WA.LCL* (e.g. **ecylan.WA.LCL**., and then click **OK**. 35. Click **OK** to close the **Identification Changes** dialog box, and then click **OK** to close the **Network Identification** message box. 36. Click **OK** to close the **System Properties** dialog box, and then click **Yes** in the **System Settings Change** message box to restart your computer.
Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS..	7. Log on as Administrator. 8. Right-click **My Network Places**, and then click **Properties**. 9. Right-click **Local Area Connection**, and then click **Properties**. 10. Click **Internet Protocol (TCP/IP)**, and the click **Properties**

	11. In the **Preferred DNS Server** text box, you're your Server IP Address, and then click **OK**. 12. Click **OK** to close the **Local Area Connections Properties** box, and then close the **Network and Dial-up Connections** window.

Step: 3

Goal: Install and configure DNS.

Tasks	Detailed Steps
Install the Domain Name System (DNS) subcomponent of Networking Services. Copy the required files from the Windows 2000 Server compact disc.	25. Logon as Administrator for your Domain 26. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Configure Your Server**. 27. Click **Networking** to expand and then click **DNS**. 28. Click **Set up DNS** on the right pane. 29. Insert the compact disc labeled Windows 2000 Advanced Server, and then click **OK**. 30. After the required files have been copied, click **Next**. 31. Expand **<MACHNAME>** 32. Right-click **<MACHNAME>** 33. Click **New Zone...** (New Zone Wizard is displayed) 34. Click **Next** 35. Click **Standard Primary** then click **Next** 36. Click **Forward Lookup Zone** then click **Next** 37. In the name field, enter **<DOMAIN-NAME>.WA.LCL** (e.g. ecytst.WA.LCL) 38. Click **Next** 39. Click **Next** 40. Click **Finish** 41. Expand **Forward Lookup Zones** 42. Right-click **<DOMAIN-NAME>.WA.LCL** 43. Click **Properties** 44. Change **Allow Dynamic Updates** to "**Yes**"

	45. Click the **Forwarders** tab select the **Enable Forwarders** check box and add the IP Addresses of the Root DNS Servers as Forwarders. 46. Click **OK** 47. Close **DNS** 48. **Restart the computer**

Step: 4

Goal: Create a Windows 2000 domain by installing Active Directory.

Tasks	Detailed Steps
Start the Active Directory Installation wizard to create: A new domain controller for a new domain. A new domain tree. A new forest of domain trees.	7. Click **Start**, and then click **Run**. 8. In the **Run** box, type **dcpromo** and then click **OK**. 9. On the **Welcome to the Active Directory Installation Wizard** page, click **Next**. 10. On the **Domain Controller Type** page, ensure **Domain controller for a new domain** is selected, and then click **Next**. 11. On the **Create Tree or child Domain** page, select **Create a new child domain in an existing domain tree,** and then click **Next**. 12. On the **Network Credentials** page, enter the username of ***<JOIN-ID>*** (e.g. ECYPromo) and password and the domain of **WA.LCL** and then click **Next**.

Complete the Active Directory installation process, providing the following information: Full DNS name of *WA.LCL* .. Default locations for the database, log files, and shared system volume.	7. On the **Child Domain Installation** page, click Browse and select **WA.LCL** to put **WA.LCL** in the Parent Domain box and ***<DOMAIN-NAME>*** in the Child Domain box and then click **Next**. 8. On the **Netbios Domain Name** page, ensure ***<DOMAIN-NAME>*** is in the Domain Netbios name box and then click **Next**. 9. On the **Database and Log Locations** page, accept the default locations by clicking **Next** 10. On the **Shared System Volume** page, accept the default location by clicking **Next**. 11. On the **Permissions** page, select **Permissions compatible with pre-Windows 2000 servers**, and then click **Next**. 12. On the **Directory Services Restore Mode Administrator Password** page, in the **Password** and **Confirm password** boxes, type in the password and then click **Next**
Begin the Active Directory Installation/Replication process ..	On the **Summary** page, review the options you selected, and then click **Next**. 3. *The Active Directory Installation/Replication process begins.* 4. When the **Completing the Active Directory Installation Wizard** page appears, click **Finish**, and then restart your computer.

Step: 5

Goal: Enable GC on your domain's first Domain Controller.

Note – A GC should not host FSMO roles.

Tasks	Detailed Steps
Enable GC.	7. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**. 8. In the console tree, expand **<DOMAIN-NAME>**, expand **servers** and then expand **<MACHNAME>**. 9. Right-click **NTDS settings** and then click **properties**. 10. Select the Global Catalog check box , and then click **OK**.

	11. Close **Active Directory Sites and Services**. 12. Reboot Computer

Step: 6

Goal: Taking Ownership of Child Domain Site and Subnet.

Tasks	Detailed Steps
Taking Ownership of the Site and Subnet that was created by the Enterprise Administrators when pre-creating the Child Domain.	15. Open the **Active Directory Sites and Services** administration tool. 16. Expand the **Sites** object. 17. Right-click your Site name and select **Properties**. 18. Select the **Security** tab. 19. Select the **Advanced** button. 20. Select the **Owner** tab. 21. Select your **Domain Admins** group in the available list and select **OK**. 22. Expand the **Subnets** folder. 23. Right-click your IP Subnet and select **Properties**. 24. Select the **Security** tab. 25. Select the **Advanced** button. 26. Select the **Owner** tab. 27. Select your **Domain Admins** group in the available list and select **OK**. 28. Close the **Active Directory Sites and Services** windows

Backing up/Restoring the Root Domain

This document is intended to present three different backup/ restore processes for the State of Washington multi-agency Forest root domain.

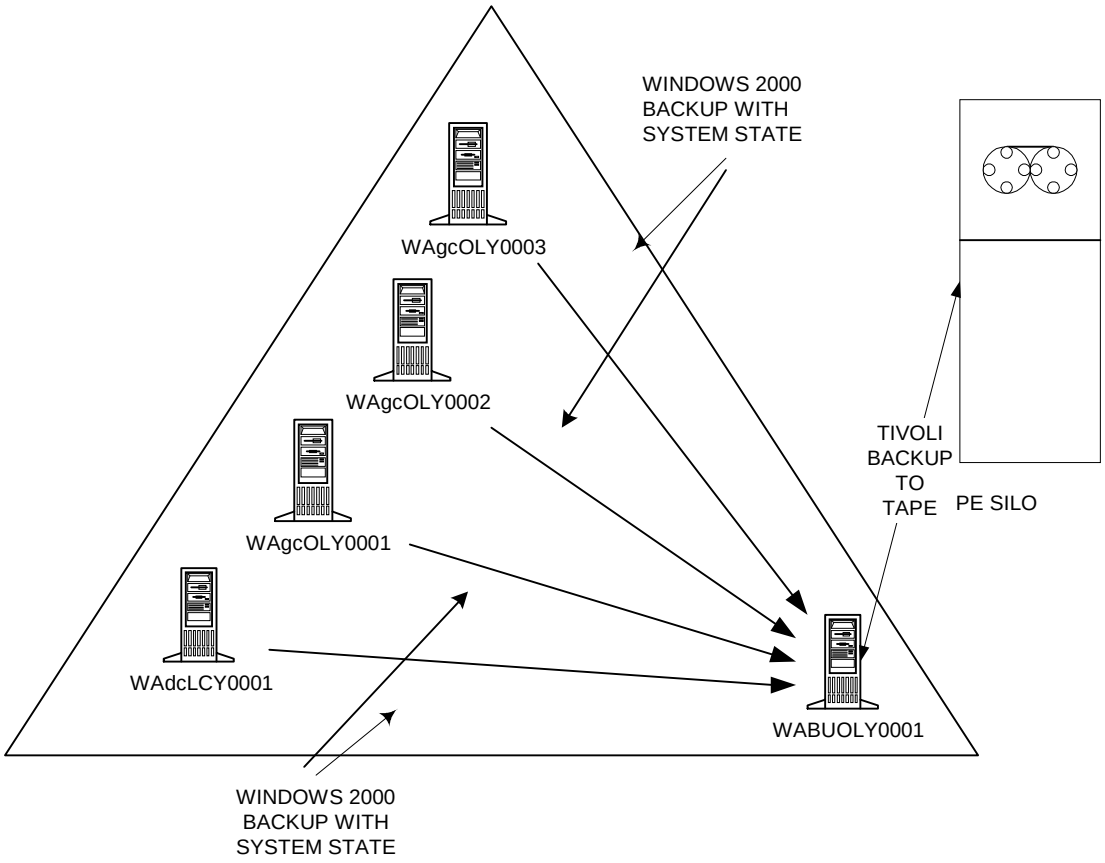
- **Loss of a Root Server**
- **Loss of Both Root Servers**
- **Authoritative restore of the Active Directory**

Backup

Backup of the Root domain controllers is done using a combination of two (2) backup processes. The first of which will be to use Windows 2000 Backup to backup the root servers and the 'natural disaster' backup server to a file on a Windows 2000 backup server including system state data. Then the backup server will be backed up to tape using Tivoli backup services from IBM. This backup service is offered by DIS to customer agencies and is also used internally by DIS for all LAN server backup.
The DIS "Server Backup Service" is part of the DIS Enterprise Storage Management Department. They provide local and off site storage, data retention management, and backup server software maintenance. In addition they include full backup images, 180 days of deleted file retention, and daily, copied backup tapes moved off site to the Redmond, Washington off site storage facility.

Following is a diagram of the topology for backing up the Root domain.

Forest Domain Backup Topology



Restore

We have two conditions which will require a restore

- Hardware failure only: Fix then restore the server from backup and let the updates to the active directory replicate.
- Hardware failure with AD corruption: Fix then restore the server from backup and mark the restored Active Directory as authoritative to fix a corruption in the Active Directory.

Backing Up and Restoring AD

To back up AD, run the Backup Wizard and select "Back up the System State Data".

On a domain controller, System State data includes:

- AD
- SYSVOL folder
- Registry
- System startup files
- Class Registration database
- Certificate Services database

You can perform the backup without taking the domain controller offline, but you can only back up the System State data for the local machine with the Win2K Backup and Recovery program.

Restoring AD

Because the AD database can't be running when you perform an AD restore, you must use a special boot mode called Directory Service Restore Mode, which you can enter by pressing F8 during the boot process. The only way to restore AD is to restore the entire System State data, which means that in addition to restoring an older copy of the directory, you also restore an older copy of the registry and therefore lose any configuration changes you made after performing the backup.

You can perform two different AD restores:

- Non-authoritative
- Authoritative.

To perform a **non-authoritative restore**:

- Boot into the Directory Service Restore Mode
- Log on using the local administrator account
- Perform a System State restore
- Reboot the system

When the system reboots, it contacts the domain controllers in the domain that are its replication partners to retrieve any updates to AD that have occurred since the backup, so you restore an AD that's a replica of the current AD on the network, not necessarily what the backup contains.

The problem is that if you accidentally delete an organizational unit (OU) from AD and you perform a non-authoritative restore, your domain controller contacts the other domain controllers on the network to retrieve any changes that have occurred, including the deletion of the OU. So how do you get your OU back? By performing an authoritative restore instead.

An **authoritative restore** is similar to a non-authoritative restore, but with an additional step. After performing the System State data restore, you use the command-line utility ntdsutil.exe to mark specific objects within the AD as authoritative.

Every AD object has a version number that changes incrementally when AD makes updates, and when you mark an AD object as authoritative, its version number increases by 100,000. When two domain controllers have different version numbers for the same object, the one with the highest version number is authoritative and replicates over the other copy of the object.

To use ntdsutil.exe to mark an object as authoritative:

1. Type **ntdsutil** at the command prompt

2. Type **authoritative restore** at the ntdsutil prompt.

To complete the restore, you need to know the distinguished name of the object or you can perform an authoritative restore of the entire directory. For example, to restore the OU that you deleted, you can use the restore subtree command and specify the OU’s distinguished name. As a final note, you can't mark the schema directory partition as authoritative, so you can't roll back schema modifications with an AD restore.

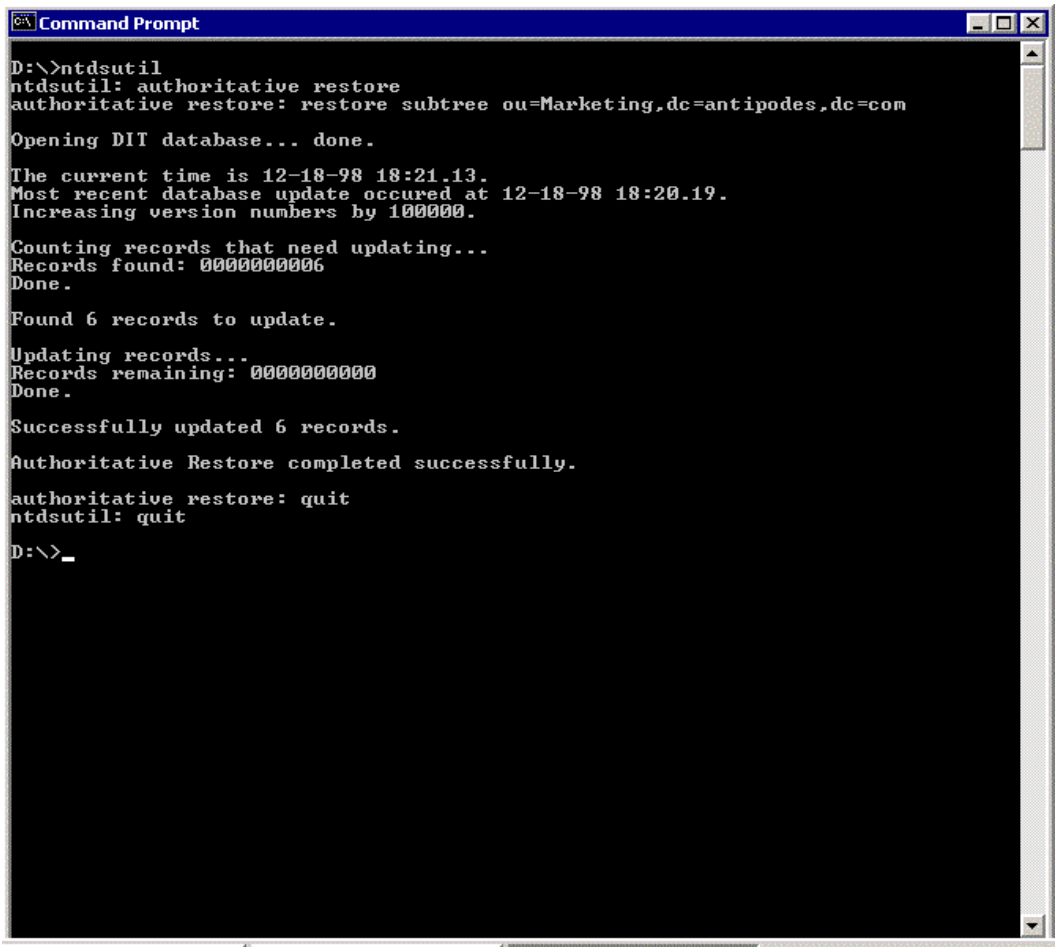
Once the restore has been completed, an optional step is to restart in Directory Service Repair Mode and verify that the Active Directory database has been restored.

The server will then be restarted into normal operational mode and the following steps will be performed automatically by the system to ensure data integrity:

- The Active Directory database files will automatically undergo a consistency check, and will be re-indexed.
- Both the Active Directory and File Replication Service will be brought up to date from their replication partners using the standard replication protocols for each of those services.

The success of the restore process can be verified by checking that the Active Directory, Certificate Server and File Replication Services are operational.

Following is a screen shot of this process.



Verification of Active Directory Restoration

Basic Verification

1. Once the restore operation has completed, the computer may be restarted into normal operational mode. The Active Directory and Certificate Server will automatically detect that they have been recovered from a backup and will perform an integrity check and re-index the database.
2. Once you can logon to the system, you should be able to browse the directory and all the user and group objects that were present in the directory prior to backup should have been restored. Similarly, files that were members of a FRS replica set and certificates that were issued by the Certificate Server should be present.

Advanced Verification

This section introduces an advanced option, which is not normally required for normal recovery operations. Incorrect usage of the utility described in this section may corrupt the Active Directory database resulting in a requirement to restore the database from backup to ensure reliable operation.

1. When restarting the server, immediately after performing the restore operation, select “Directory Service Repair Mode” from the boot menu.
2. Once the system has started, login with the standalone server’s administrator account.
3. Verify that the Active Directory is in a state consistent with having been recovered from a backup. This is done by checking for a specific registry key. Start RegEdit. Click **Start,** then click **Run**, type in **regedit** then click **OK.**
4. Select the registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS** Check that there is a subkey called **“Restore In Progress”.** This key is automatically generated by NT Backup and indicates to the Active Directory Service that the database files have been restored and a consistency check and re-index should be performed the next time the directory is started. This key is automatically removed upon completion of this check.
   DO NOT ADD or DELETE this key manually.

5. Check for the recovered Active Directory database files with the utility "NTDSUTIL" Click **Start,** then click **Programs**, then click **Command Prompt**.

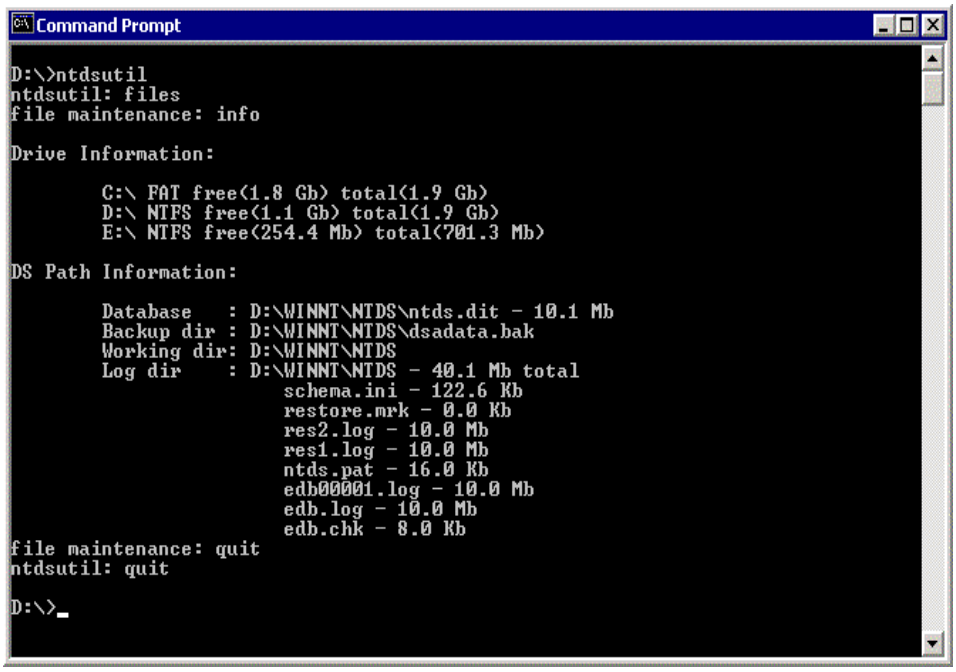
    a. Start NTDSUTIL at the Command Prompt.

    b. At the command prompt type **NTDSUTIL.**

    c. At the NTDSUTIL prompt type **files.**

    d. At the file maintenance prompt type **info.**

    If the Active Directory files have been recovered successfully it will list information similar to that shown below.
    DO NOT SELECT ANY OTHER OPTIONS



6. Once you have confirmed that the Active Directory has been restored from the backup and that the registry keys are present, then simply restart the server in normal mode.
7. When the computer is restarted in normal mode the Active Directory will automatically detect that it has been recovered from a backup and will perform an integrity check and re-index the database.
8. Once you can logon to the system, you should be able to browse the directory and all the user and group objects that were present in the directory prior to backup should have been restored.

Appendix

Best practices for Windows 2000 DNS Servers

- **Enter the correct e-mail address of the responsible person for each zone you add to or manage on a DNS server.**

  This field is used by applications to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. While most Internet e-mail addresses contain the at sign (**@**) when used in e-mail applications, this symbol must be replaced with a period (**.**) when entering an e-mail address for this field. For example, instead of "example@microsoft.com", you would use "example.microsoft.com".

  For more information on configuring the responsible person for a zone, see To modify the start of authority (SOA) record for a zone

- **Be conservative in adding alias records to zones.**

  Avoid using CNAME resource records (RRs) where they are not needed to alias a host name used in a host (A) resource record. Also, ensure that any alias names you use are not used in other RRs. For example, if you want to use a CNAME RR to support an alias name of "alias.example.microsoft.com", you would not use the first name label ("alias") in other RRs for the "example.microsoft.com" zone.

  Windows 2000 DNS permits you to repeat a name label used in other types of resource records (such as NS, MX, or TXT records) at the same domain level in the namespace tree. As per the Request for Comments (RFCs) guidelines, CNAMEs are expected to follow a sectional processing scheme in which they resolve an aliased host name submitted as a query to mapped host names as stated in other host (A) resource records. For standard and expected resolution of CNAMEs, you must administer your zones manually to enforce uniqueness of names for RRs used to support this process.

  For more information, see Alias (CNAME) resource records

- **When designing your DNS network use standard guidelines and, wherever possible, follow preferred practices for managing your DNS infrastructure.**

  DNS was designed to provide a level of fault tolerance for resolving names. If possible, you should have at least two name servers hosting each zone.

Server best practices

For the routine management and administration of servers that you operate on your network using the DNS service, the following guidelines should be considered and used as appropriate to your DNS deployment:

- **If you are using Active Directory, use directory-integrated storage for your zones for best results and simplified deployment and troubleshooting.**

  Note: This applies to the Forest Root; application to an agency Domain Controller is at the discretion of the agency.

  By integrating zones, you can simplify network planning. For example, domain controllers for each of your Active Directory domains correspond in a direct one-to-one mapping to DNS servers. This can simplify planning and troubleshooting DNS and Active Directory replication problems because the same server computers are used in both topologies.

  If your DNS client computers are running Windows 2000, configuring them to perform dynamic updates in DNS can also be simplified. For example, when configuring a list of preferred and alternate DNS servers for each client to use, you only need to use server IP addresses corresponding to domain controllers located near each client. If a client should fail to update with its preferred server (because the server is unavailable), an alternate server can be tried instead. This permits the client to successfully update its records at another server that loads the directory-integrated DNS zone.

- **If you are not using Active Directory, be aware of the points of failure and configuration issues that apply to using dynamic updates with standard primary type zones.**

  Standard primary type zones are required to create and manage zones in your DNS namespace if you are not using Active Directory. In this case, a single-master update model applies, with one DNS server designated as the primary server for a zone. Only the primary server, as determined in the SOA record properties for the zone, can process an update to the zone.

  For this reason, be certain that clients are configured to use a preferred DNS server that is reliable and available to process and refer updates. Otherwise, clients are not able to successfully update their host (A) or pointer (PTR) resource records (RRs).

- **Consider the use of secondary or caching-only servers for your zones to assist in off-loading DNS query traffic wherever it makes sense.**

  Secondary servers can be used as backups for DNS clients or as the preferred DNS servers for legacy DNS clients. For mixed-mode environments, this allows you to use secondary servers as a means to load balance DNS query traffic on your network, and reserve your DNS-enabled primary servers for use only by those clients that need them to perform dynamic registration and updates of their A and PTR RRs.

  For more information on the use of secondary or caching-only servers, refer to the following sections.

Internet DNS best practices

The Internet Engineering Task Force (IETF) has published several Request for Comment (RFC) documents that cover best practices for DNS, as recommended by various DNS architects and planners for the Internet. It is useful to review these

RFCs, particularly if you are planning a large DNS design, such as for a large Internet service provider (ISP) that supports the use of DNS name service.
Current RFCs that cover Internet DNS best practices include those listed in the following table.

RFC	Title
1912	Common DNS Operational and Configuration Errors
2182	Selection and Operation of Secondary DNS Servers
2219	Use of DNS Aliases for Network Services

You can obtain these RFCs from the Request for Comments Web site. This Web site is currently maintained by members of the Information Sciences Institute (ISI) who publish a classified listing of all RFCs. RFCs are classified as one of the following: approved Internet standards, proposed Internet standards (circulated in draft form for review), Internet best practices, or For Your Information (FYI) documents.
To see the most current RFCs related to actively defining the DNS standard, use the following links to refer to the appropriate Active IETF Working Groups Web sites:

- DNS incremental zone transfer (IXFR), notification, and dynamic update
- DNS operations
- DNS security

Note

- Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.